AEROSPACE SAFETY ADVISORY PANEL

National Aeronautics and Space Administration

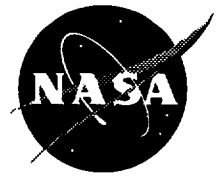
ANNUAL REPORT FOR 1997

"THE PANEL shall review safety studies and operations plans referred to it and shall make reports thereon, shall advise the Administrator with respect to the hazards of proposed or existing facilities and proposed operations and with respect to the adequacy of proposed or existing safety standards and shall perform such other duties as the Administrator may request."

(NASA Authorization Act of 1968, Public Law 90-67, 42 U.S.C. 2477)

National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001



Reply to Attn of: Q-1

February 1998

Honorable Daniel S. Goldin
Administrator
National Aeronautics and Space Administration
Washington, DC 20546

Dear Mr. Goldin:

The Aerospace Safety Advisory Panel herewith presents its annual report documenting the Panel's activities for calendar year 1997. We would appreciate NASA's response to the findings and recommendations in Section II.

This year was a period of consolidation within NASA. Transition to the Space Flight Operations Contract (SFOC) initiated near the end of 1996 gained momentum during 1997. Many of the less critical tasks and processes and a few of the more critical ones formerly done by NASA were transferred to the United Space Alliance. Thus far, Space Shuttle operations under the SFOC have proceeded smoothly and safely as indicated by the record of flight successes.

The Panel firmly believes that NASA and its contractors are presently maintaining a commitment to "safety first." We are not quite as comfortable about the future. The competitive situation in the aerospace marketplace is making the retention of experienced and skilled workers difficult at best. Budget appropriations and their allocations are forcing continued staff reductions that have little relationship to workload. Together with hiring freezes, these staff shortfalls will inevitably hamstring NASA's ability to monitor adequately the performance of Space Shuttle operations. The Panel will continue to observe closely any safety implications of these circumstances.

The delay of the launch of the first International Space Station (ISS) element was a prudent management decision. The schedule was extremely tight and quite probably would have caused workarounds and shortcuts that could have been extremely detrimental to safety. Although the delay did permit some flexibility, the schedule is still very success oriented. The Panel will watch preparations for the launch of the ISS with great interest.

The Panel is grateful to all NASA and contractor personnel for their cooperation and assistance during the past year.

Very truly yours,

Richard D. Blomberg for/

Paul M. Johnstone
Chairman
Aerospace Safety Advisory Panel

This year, the Aerospace Safety Advisory Panel lost two of its own. First, on October 5, **Patricia M. Harman**, our long-time Staff Assistant, succumbed to a protracted illness. Throughout her career, Pat brought a "can do" spirit to her job. She continued to work until the end in spite of her illness, providing outstanding service to the Panel. Everyone she touched will remember Pat as a dedicated contributor with a true passion for NASA's mission and America's space program.

Just as the sorrow of Pat's passing began to subside, we were shocked by the sudden death of our Chairman, **Paul M. Johnstone**, on December 17. Paul was a true giant in the aerospace industry. Whether as an aircraft designer leading the engineering department of a major airline, guiding the Panel, or as a Fellow of the American Institute of Aeronautics and Astronautics, Paul's firm but fair hand, keen insights, and good humor invariably produced superior results. As the Panel's leader, he was adept at ensuring that we were properly focused and that each individual member's capabilities were used to their maximum potential.

Paul and Pat were our friends and colleagues. They were an irreplaceable part of our lives. We will always remember and be grateful for the time we spent with them and the contributions they made to our lives and our organization. We dedicate this report to them as a small token of our esteem.

National Aeronautics and
Space Administration

AEROSPACE SAFETY ADVISORY PANEL

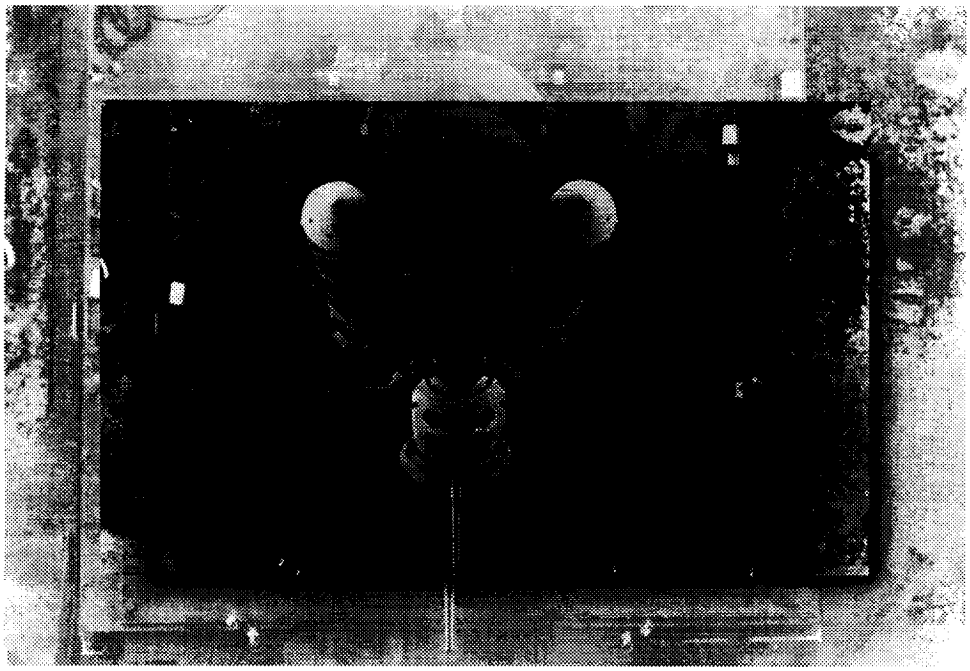
ANNUAL REPORT FOR 1997

February 1998

Aerospace Safety Advisory Panel
Code Q-1
NASA Headquarters
Washington, DC 20546
Tel: 202 / 358-0914

Table of Contents

I. Introduction



I. Introduction

During 1997, the Aerospace Safety Advisory Panel (ASAP) continued its safety reviews of NASA's human space flight and aeronautics programs. Efforts were focused on those areas that the Panel believed held the greatest potential to impact safety. Continuing safe Space Shuttle operations and progress in the manufacture and testing of primary components for the International Space Station (ISS) were noteworthy.

The Panel has continued to monitor the safety implications of the transition of Space Shuttle operations to the United Space Alliance (USA). One area being watched closely relates to the staffing levels and skill mix in both NASA and USA. Therefore, a section of this report is devoted to personnel and other related issues that are a result of this change in NASA's way of doing business for the Space Shuttle. Attention will continue to be paid to this important topic in subsequent reports.

Even though the Panel's activities for 1997 were extensive, fewer specific recommendations were formulated than has been the case in recent years. This is indicative of the current generally good state of safety of NASA programs. The Panel does, however, have several longer term concerns that have yet to develop to the level of a specific recommendation. These are covered in the introductory material for each topic area in Section II.

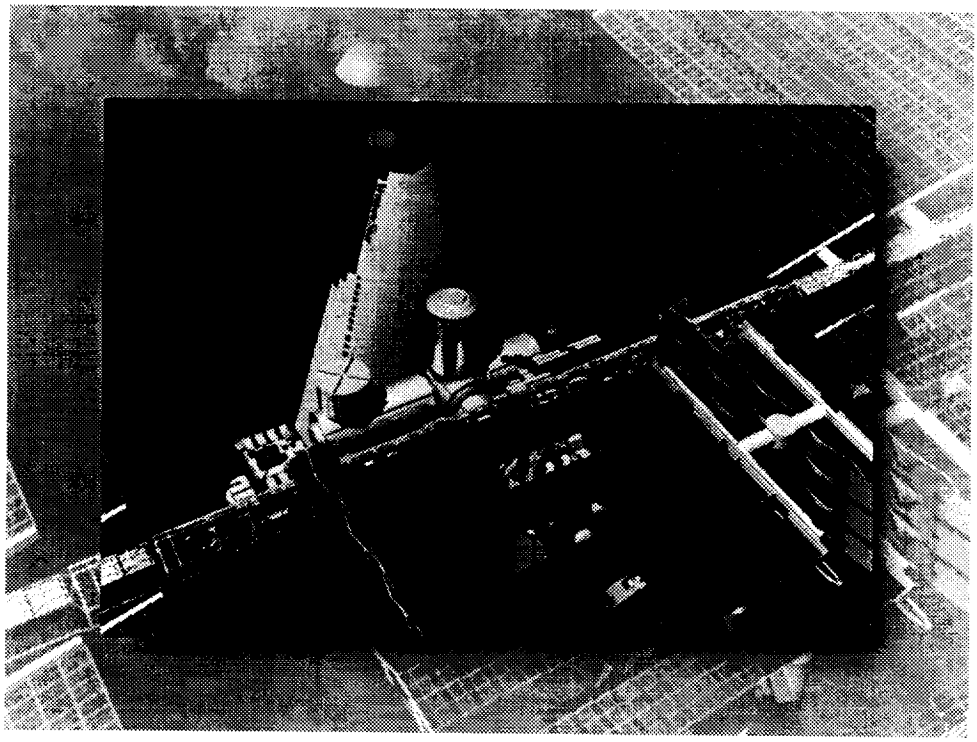
In another departure from past submissions, this report does not contain individual findings and recommendations for the aeronautics programs. While the Panel devoted its usual efforts to examining NASA's aeronautic centers and programs, no specific recommendations were identified for inclusion in this report. In lieu of recommendations, a summary of the Panel's observations of NASA's safety efforts in aeronautics and future Panel areas of emphasis is provided.

With profound sadness the Panel notes the passing of our Chairman, Paul M. Johnstone, on December 17, 1997, and our Staff Assistant, Ms. Patricia M. Harman, on October 5, 1997.

Other changes to the Panel composition during the past year were: the resignation of Mr. Dennis E. Fitch as a Consultant; the appointment of Mr. Roger D. Schaufele as a Consultant; and the assignment of Ms. Susan M. Smith as Staff Assistant.

The balance of this report presents "Findings, Recommendations, and Observations" (Section II), "Information in Support of Findings, Recommendations, and Observations" (Section III), and Appendices (Section IV) listing Panel membership, the NASA response to the February 1997 ASAP report, and a chronology of the Panel's activities during the reporting period.

II. Findings, Recommendations, and Observations



II. Findings, Recommendations, and Observations

II. Findings, Recommendations, and Observations

A. SPACE SHUTTLE PROGRAM

In general, the Space Shuttle systems performed well during 1997. There were, however, some in-flight anomalies and development test failures. Among the more significant of these were: the fuel cell performance uncertainty on STS-83; the nozzle throat erosion of the Reusable Solid Rocket Motors (RSRMs) on several flights; the failure of the Space Shuttle Main Engine (SSME) Number 0524 during a development test of the Block II configuration; and the omission of critical washers on the ferry flight of *Atlantis* (OV-104) to Palmdale for its Orbiter Maintenance and Down Period (OMDP).

The Panel tracked the analysis and resolution of these incidents via indepth fact-finding with both NASA and contractor installations. It was concluded that the investigation to determine the cause of each incident was carried out by all parties in scrupulous and tenacious adherence to the standing procedures established by NASA and its contractors. When extensive testing was conducted to establish and verify cause(s), the testing appeared to be warranted and appropriately conducted. Those incidents that were closed were characterized by implementing appropriate corrective action(s) involving both procedural and design changes as needed. All told, NASA's response to the incidents and resolution of the causes identified to date reflected high professionalism and adherence to the policy of "safety first, schedule second."

The SSME program continued the development of the Block II configuration, which should be a major safety improvement. The Panel has favored the continued testing of the Block II engine after its certification in order to define its true operating limits. This could lead to the certification of a higher power setting for use in aborts and would improve safety.

Another area of major Space Shuttle activity relates to the organization of and responsibilities for Space Shuttle operations. The transition to a single prime contractor under the Space Flight Operations Contract (SFOC) continued smoothly. NASA and the SFOC contractor also began examinations of privatization of the Space Shuttle operations. Although these efforts have not created any immediate safety concerns, the long-range implications of declining personnel numbers and

potential skill mix imbalances are being watched. These issues are discussed more fully in a separate section of this report.

The general state of the Integrated Logistics System (ILS) is healthy despite the need for continuing tradeoffs. Examination of statistics shows that all the measurement parameters, such as problem reports, component repair summaries, shelf stock status, and scheduled and unscheduled maintenance actions, are at a satisfactory level. The principal concerns are cannibalization, component repair and turnaround times, and loss of spares available due to obsolescence and vendors going out of business.

The "integrated management" of the logistics and support programs under the United Space Alliance (USA) appears to be working very well, and the extensive backgrounds and administrative experience of the senior personnel result in a cohesive and forward-looking concept. Continuity for the next working generation of management appears to be high on the list of management priorities.

OPERATIONS/PROCESSING

Finding #1

Operations and processing in accordance with the Space Flight Operations Contract (SFOC) have been satisfactory. Nevertheless, lingering concerns include: the danger of not keeping foremost the overarching goal of safety before schedule before cost; the tendency in a success-oriented environment to overlook the need for continued fostering of frank and open discussion; the press of budget inhibiting the maintenance of a well-trained NASA presence on the work floor; and the difficulty of a continued cooperative search for the most meaningful measures of operations and processing effectiveness.

Recommendation #1a

Both NASA and the SFOC contractor, USA, should reaffirm at frequent intervals the dedication to safety before schedule before cost.

Recommendation #1b

NASA should develop and promulgate training and career paths leading to qualification for senior NASA Space Shuttle management positions.

Recommendation #1c

NASA should continue to ensure that a trained and qualified Government personnel presence is maintained on the work floor.

Recommendation #1d

NASA and USA should continue to search for, develop, test, and establish the most meaningful measures of operations and processing effectiveness possible.

Finding #2

The Kennedy Space Center (KSC) has been successfully phasing in the structured surveillance process for safety and quality for some time. The development of metrics using structured surveillance information has lagged data collection.

Recommendation #2

KSC should continue to expand the use of structured surveillance and to focus effort on the development of valid and reliable metrics to assess program performance from structured surveillance results.

Finding #3

NASA Safety and Mission Assurance (S&MA) auditors at KSC overseeing operations requiring Self-Contained Atmospheric Protective Ensemble (SCAPE) are not certified for SCAPE.

Recommendation #3

In order to be in a position to conduct valid safety and quality audits of SCAPE operations, NASA should ensure that personnel involved are certified so that, when necessary, they can observe the tasks while they are performed.

Finding #4

To compensate for skills deficiencies related to staff departures from KSC, both NASA and USA are making extensive use of cross-training of personnel, both technicians and engineers. Individuals who have been cross-trained also should have recent "hands-on" experience before they undertake a cross-trained task.

Recommendation #4

NASA and USA should develop and use valid and reliable measures of the readiness of personnel to take on tasks for which they have been trained but on which they have only limited or episodic experience. The cross-training program could include a regularly scheduled rotation of duties so that the multiply trained individual has the opportunity to employ all of the acquired skills and knowledge at appropriate intervals.

Finding #5

The reduction of Government Mandatory Inspection Points (GMIPs) at KSC has significantly lagged the downsizing of NASA quality personnel responsible for processing these GMIPs. This has resulted in an expanded workload among remaining NASA quality inspectors and made it more difficult to conduct analyses needed to identify further GMIP reductions. There has been a similar reduction of NASA safety inspectors and engineers at KSC without a commensurate reduction in oversight requirements while, at the same time, the addition of new safety audit or insight responsibilities has taken place.

Recommendation #5

Any downsizing of personnel by both NASA and USA should be preceded by the reduction of commensurate workload associated with Space Shuttle processing, such as reduction of GMIPs and NASA safety inspections.

EXTERNAL TANK (ET)

Finding #6

The Super Light Weight Tank (SLWT) has completed its design certification review, and proof tests on the first tank have been satisfactorily passed. The only remaining test to complete certification of the SLWT is the cryogenic loading test that will be run on the first production tank on the launch pad. The diligent attention that has been given to quality control, particularly to material inspection and weld integrity, has made this program successful.

Recommendation #6

NASA should ensure that the current manufacturing and quality control procedures continue to be rigidly adhered to and conscientiously followed in production.

Finding #7

The design requirements for the SLWT include operating with a maximum Space Shuttle Main Engine (SSME) power of only 106%, even at abort conditions. The Space Shuttle program has approved a baseline plan to examine the possibility of certifying the Space Shuttle for intact aborts at a 109% SSME power setting.

Recommendation #7

NASA should complete its evaluation of a 109% power setting for intact aborts as soon as practicable and reevaluate the ability of the SLWT to accommodate this higher power setting.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Finding #8

Obsolescence changes to the RSRM processes, materials, and hardware are continuous because of changing regulations and other issues impacting RSRM suppliers. It is extremely prudent to qualify all changes in timely, large-scale Flight Support Motor (FSM) firings prior to produce/ship/fly. NASA has recently reverted from its planned 12-month FSM firing interval to tests on 18-month intervals.

Recommendation #8

Potential safety risks outweigh the small amount of money that might be saved by scheduling the FSM motor tests at 18-month intervals rather than 12 months. NASA should realistically reassess the test intervals for FSM static test firings to ensure that they are sufficiently frequent to qualify, prior to motor flight, the continuing large number of materials, process, and hardware changes.

LOGISTICS

Finding #9

Support of the Space Shuttle fleet with operational spares has been maintained by the effective efforts of the logistics function. While spares support has been adequate for the current flight rate, any increase in flight rate might not be supportable.

Recommendation #9

Although NASA has established programs for dealing with suppliers and bringing additional component overhaul "in house," efforts in these areas need to be continuously reexamined to speed up the restoration and upgrading of line-replaceable units. Such efforts are especially needed to eliminate "dead" time while units are awaiting restoration.

Finding #10

Transition and development of the logistics tasks for the orbiter and its ground operations under the SFOC are proceeding efficiently and according to plan.

Recommendation #10

NASA and USA should continue the task of management integration of the formerly separate logistics contracts and retain and expand the roles of the experienced logistics specialists therein.

Finding #11

As reported last year, long-term projections are still suggesting increasing cannibalization rates, increasing component repair turnaround times, and loss of repair capability for the Space Shuttle logistics programs. If the present trend is not arrested, support difficulties may arise in the next 3 or 4 years.

Recommendation #11

NASA and USA should reexamine and take action to reverse the more worrying trends highlighted by the statistical trend data.

B. INTERNATIONAL SPACE STATION (ISS) PROGRAM

The start of deployment of the ISS was delayed because of problems in the delivery of the Russian-built Service Module. The additional development time is being used by NASA to permit some integrated testing of modules at KSC before launch. This testing is an excellent step that should improve both the safety and operability of the station on-orbit. The additional time is also fortuitous for the development of software and the caution and warning system that are behind schedule. Details on software issues are presented in a separate section of this report.

The handling of meteoroid and debris risks to the ISS progressed well during the year, although the processes for collision avoidance and maneuvering are still not finalized. The development of the X-38 vehicle that is intended to become the basis for a Crew Return Vehicle (CRV) also moved ahead. The CRV development schedule, however, is extremely optimistic. Any delay in the operational date for NASA's CRV will mean a longer reliance on Soyuz capsules and attached Space Shuttles. This will constrain ISS operations and may lead to safety problems. It is important for the long-term safety of the ISS that a realistic CRV design and deployment schedule be finalized as soon as possible. This will permit operational plans to be devised that adequately take into account issues such as the service life of the Soyuz.

Finding #12

Node #1 was shipped to KSC before completion, and it is planned or anticipated that other ISS hardware will be shipped before qualification tests are completed. This disrupts the desirable continuity of effort and can lead to safety problems.

Recommendation #12

NASA should ensure that ISS assemblies shipped before completion of the manufacturing, testing, and qualification processes have been carefully scrutinized to make sure that no safety-related steps are subverted.

Finding #13

The ISS Phase I Shuttle-Mir program has reaffirmed what was learned on Skylab: that a manned space station can be surprisingly resilient in emergency situations. Much has been learned from the operations on Mir to date and much more may be learned from continued analysis of joint operations on Mir.

Recommendation #13

The ISS team should continue to examine the Shuttle-Mir program carefully for examples from which ISS operations can benefit and to provide policies and procedures to implement effective action should similar events occur on the ISS. The effort should be expanded beyond Mir to focus as well on possible weaknesses in the ISS design and operations. The ISS should assemble a special team, including persons with system-level perspectives as well as with design, operations, and human factors experience, to address these issues.

Finding #14

Radiation exposures of U.S. astronauts recorded over several Mir missions of 115 to 180 days duration have been approximately 10.67 to 17.20 REM. If similar levels of exposure are experienced during ISS operations, the cumulative effects of radiation could affect crew health and limit the number of ISS missions to which crewmembers could be assigned.

Recommendation #14

Determine projected ISS crew radiation exposure levels. If appropriate, based on study results, initiate a design program to modify habitable ISS modules to minimize such exposures or limit crew stay time as required.

Finding #15

Although considerable progress has been made during this past year in ISS Caution and Warning (C&W) system design, systems engineering is still not sufficiently evident in the whole spectrum of alarm and warning, situation assessment, and damage control and repair.

Recommendation #15

Initiate a high-priority systems engineering review of the C&W system to define a path for development and implementation of fully integrated alarm, situation assessment, countermeasure functions and crew actions. Finalize and document C&W system design requirements.

C. COMPUTER HARDWARE/SOFTWARE

Software is a major safety-critical part of both the Space Shuttle and ISS. Its development also represents a significant determinant of schedule and cost. Although much progress has been made in the software development processes used and in the coding of the various software products themselves, the Panel retains several concerns. These are reflected in the specific findings and recommendations below.

Finding #16

The ISS software development schedule is almost impossibly tight. If something else does not cause a further delay in ISS deployment, software development may very well do so. The decision this year to add integrated testing of some modules at KSC is a very positive step for safety. However, there is no room in the schedule for required changes that may be discovered during this testing.

Recommendation #16

NASA should realistically reevaluate the achievable ISS software development and test schedule and be willing to delay the ISS deployment if necessary rather than potentially sacrifice safety.

Finding #17

NASA does not yet have adequate plans for the long-term maintenance of the software development tools being used to produce the ISS software.

Recommendation #17

NASA should recognize the importance of maintaining its software development tools, plan now for how these are to be maintained over a period of decades, and provide adequate funding to support this activity.

Finding #18

The computer system being developed for the ISS is already at a point where NASA should begin planning for upgrading it. The ISS program presently has no plans for upgrading the ISS computer system.

Recommendation #18

NASA should upgrade the ISS computer system as soon as possible and coordinate the upgrade with its solution to the long-term development tool maintenance problem.

Finding #19

The Checkout and Launch Control System (CLCS) program at KSC has not been provided with funding for Independent Verification and Validation (IV&V) that is safety critical for a software effort of this size.

Recommendation #19

The CLCS should be provided with adequate funding for software IV&V.

D. AERONAUTICS AND SPACE TRANSPORTATION TECHNOLOGY

The NASA Aeronautics and Space Transportation Technology Enterprise places great emphasis on safety of its flight programs while striving to increase significantly the effectiveness and competitiveness of U.S. aviation, both civil and military. There is greatly increased cooperation with the Federal Aviation Administration (FAA) to update the Nation's air traffic management capabilities and to begin new initiatives directed at significantly increasing safety of civil aviation. The emphasis on better and more timely weather information for the flight deck along with the error-proof digital avionics effort would appear to be absolutely necessary elements of the accident reduction effort.

There are also many ongoing technology projects, such as aging aircraft and crack detection, the Advanced General Aviation Transport Experiments (AGATE), aircraft noise reduction, tire traction testing, and icing research, that contribute to increased safety. The High Speed Research program includes atmosphere and propulsion research for defining requirements for future supersonic civil transport aircraft. These technology advancement programs often lead to flight experiments at the Dryden Flight Research Center (DFRC).

The airworthiness and flight readiness process at DFRC is excellent and truly places heavy emphasis on the principle of safety first and mission schedule second. This is necessary because there are several flight programs at DFRC that have inherent safety risks that deserve special emphasis. These include: the Linear Aerospike SR-71 Experiment (LASRE); the F-106 Eclipse; and the Pathfinder solar-powered unoccupied air vehicle.

The X-33 and X-34 flight research vehicles are laying the groundwork for future space transportation systems. Because the X-33 extended range flight tests will involve flight over populated areas, the Panel will pay close attention to the plans for these flights.

The Panel is concerned that a second (research) cockpit is not being installed in the Boeing 757 at the Langley Research Center due to funding constraints. The safety enhancements that may be derived from testing with this modification should be re-evaluated.

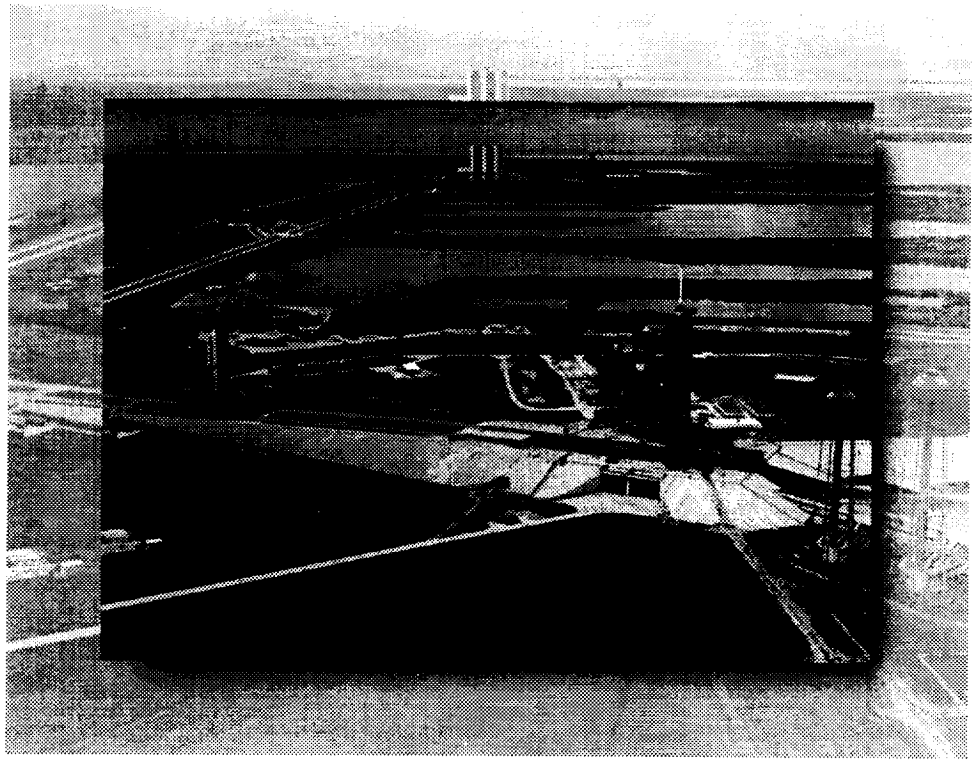
E. PERSONNEL

The continuing downsizing of NASA personnel has the potential of leading to a long-term shortfall of critical engineering and technical competencies. Nonetheless, the record of the agency in 1997 has been impressive with a series of successful Space Shuttle launches on time and with a minimum of safety-related problems. However, further erosion of the personnel base could affect safety and increase flight risk because it increases the likelihood that essential work steps might be omitted. Also, the inability to hire younger engineers and technicians will almost surely create a future capabilities problem.

Among the Panel's concerns are:

- Lack of Center flexibility to manage people within identified budget levels rather than arbitrary personnel ceilings
- Erosion of the skill and experience mix at KSC
- Lack of a proactive program of training and cross-training at some locations
- Continuing freeze on hiring of engineers and technical workers needed to maintain a desirable mix of skills and experience
- Difficulty of hiring younger workers (e.g., co-op students and recent graduates)
- Staffing levels inadequate to pursue ISO 9000 certification

III. Information in Support of Findings, Recommendations, and Observations



III. Information in Support of Findings, Recommendations, and Observations

A. SPACE SHUTTLE PROGRAM

OPERATIONS/PROCESING

Ref: Finding #1

Neither the United Space Alliance (USA) nor NASA has yet laid to rest the perception among NASA employees that the bottom-line requirement of the contractor to make a profit will, in the end, prompt the contractor to take shortcuts and compromise safety. This perception exists at all ranks, from astronauts through engineers to quality people on the work floor.

There is considerable evidence that the current outstanding cooperation between NASA and contractor personnel is the product of long years of association. For example, frank and open discussion is now the norm in NASA/contractor relationships. Unfortunately, it is not clear that there are definitive plans for ensuring that such relationships will continue to exist when the current generation of NASA and contractor managers leaves the program.

Presence on the work floor is key to gaining true insight into contractor practices. In addition, the Space Shuttle program's excellent safety record is due in large part to the presence of knowledgeable people on the work floor. Any change in this presence must be carefully considered.

Presently established measures of effectiveness for contractor performance appear for the most part to be adequate, but they tend to be measures of the "low hanging fruit." Other more meaningful measures are undoubtedly available; they just have to be discovered. A program to do that must be pursued with vigor.

Ref: Finding #2

The Kennedy Space Center (KSC) and its contractors began using structured surveillance several years ago on low criticality tasks. The idea was to conserve resources and remove the Government from direct involvement in operational tasks by placing the responsibility for quality and safety directly on the technician performing the work. The approach has worked well in other industries, particularly airlines.

Now that there is significant experience with the structured surveillance approach, a cautious expansion appears warranted. This expansion could possibly encompass more low criticality ("crit 3") tasks as well as selected tasks of higher criticality. Valid and reliable metrics to indicate how well the structured surveillance approach is achieving its goals are needed. These metrics do not yet exist. Their development and validation should precede any extension of structured surveillance beyond its present focus on low criticality tasks that are routinely verified during a subsequent activity.

Ref: Finding #3

As NASA has downsized its staff at KSC, it has not been possible to control totally the composition of staff departures. This has reduced technical capabilities in some critical areas. As a result, the Safety and Mission Assurance (S&MA) Office does not have anyone qualified in Self-Contained Atmospheric Protective Ensemble (SCAPE) operations. At the time of the Panel's review, the S&MA personnel assigned to assessing SCAPE operations had not had any firsthand experience with SCAPE and were not SCAPE certified so they could not witness these operations. This means that S&MA's structured surveillance (when it is fully operational) will not be able to cover SCAPE activities effectively. Working with reactive propellants is a hazardous operation that requires training and experience. It is likely that some SCAPE experience is required in order to be an effective auditor of a SCAPE operation.

To counter this problem, NASA should enumerate the safety-critical operations that must be audited. Every effort should then be made to retain or engage NASA personnel for S&MA audit activities who are trained and experienced in the defined safety-critical activities. If this is not possible, existing personnel should be trained in the operation being audited. This will help ensure that the audit activities are as effective as possible in validating the processes used by the contractor.

Ref: Finding #4

As a result of unplanned departures of personnel, both NASA and USA at KSC are experiencing a shortfall of skills in some critical areas. To compensate, both the government and the contractor have instituted cross-training programs. These types of efforts have a great potential for compensating for temporary skill imbalances. Personnel who are scheduled for cross-training probably already have an excellent understanding of overall Space Shuttle systems.

One potential problem with cross-training is that training itself is usually not a complete substitute for thorough and recent experience. Thus, cross-trained personnel may still not be fully ready to step into an assignment in their new area of competence. At present, there are no good indicators of the readiness of cross-trained personnel to step into a different position. The development of such readiness indicators would add greatly to the confidence management could have in utilizing these

cross-trained people. Until valid indicators are available, cross-trained people should be used in safety-critical situations only if there is adequate supervision. It would also be beneficial to develop a regular rotation of the cross-trained workforce among all of the specialties for which they are prepared to provide "hands-on" experience. This will help ensure appropriate readiness as well as sufficient training.

Ref: Finding #5

In prior reports, the Panel has cautioned that reductions in NASA and USA personnel should not outdistance the reductions in workload associated with those positions. Nonetheless, in a transition of the magnitude currently taking place in terms of downsizing and the shift of processing responsibilities from NASA to USA, it is not surprising that these relationships will on occasion get out of phase.

For example, the continuing downsizing of NASA space flight center personnel, in conjunction with the shift of NASA responsibilities under the SFOC from active involvement in Space Shuttle processing to one of providing "insight," assumes a significant reduction of Government Mandatory Inspection Points (GMIPs). Unfortunately, this GMIP reduction has been progressing very slowly. As a result, the reduced NASA personnel are having to process virtually as many GMIPs as they did when prior employment levels were in place. This continuing high workload, in many instances, has made it difficult to conduct the analyses that are required to identify GMIPs that can be safely eliminated.

The transition to the SFOC has also placed more responsibility for job site safety on the technicians themselves. The approach of making the touch labor workforce responsible for safety without the direct involvement of NASA or USA inspectors has proved effective in analogous environments. However, implementing this approach at KSC should take account of several unique challenges. First, there is a heritage of multiple inspections and direct oversight by NASA and contractor personnel. Thus, the shift to structured safety approaches is a significant departure. Second, the shift is taking place simultaneously with significant downsizing by both NASA and USA. Third, the reduction in oversight duties for NASA inspectors has been somewhat delayed while audit or "insight" duties have been added. Fourth, attrition of NASA safety personnel has left the Government workforce shorthanded to accomplish both GMIPs and insight tasks.

It is probable that problems or upsets due to these unique factors are not permanent and will dissipate as personnel gain greater familiarity with the new approach to Space Shuttle processing. In the interim, NASA and contractor management should be sensitive to the potential for transitional problems and remain vigilant. This must involve assessments of metrics and a continuing direct involvement on the work floor. It is also desirable to maintain active communications with the workforce on the progress of the transition efforts.

EXTERNAL TANK (ET)

Ref: Finding #6

The proof test of the new Super Light Weight Tank (SLWT) consists of a series of stress tests run at room temperature, with some of the stresses in the tank walls at levels less than will be experienced in flight. The predicted improvement in material properties at cryogenic temperatures is then used to show that flight stresses will be acceptable. This is the same approach that has been used successfully on all prior external tanks for the Space Shuttle. There is, however, a significant difference from the previous external tanks in that most of the SLWT is made from 2195 aluminum-lithium alloy. This alloy has unique material properties and has had far less operating experience than the 2219 aluminum alloy used on all previous external tanks.

Welding procedures (including repair techniques) for the 2195 aluminum-lithium alloy have been successfully developed and demonstrated on a test article and on the first production units. These procedures are different and less forgiving than those used for the 2219 alloy and must be followed very carefully. The External Tank Project at Marshall Space Flight Center and the contractor are well aware of these concerns. Full support for their continued oversight of production is warranted.

Ref: Finding #7

The Block II Space Shuttle Main Engine (SSME) is being certified to operate at 104.5% power setting for most of the International Space Station (ISS) missions, at 106% for a few ISS missions with heavy payloads, and at 109% for abort. The abort mode would be required, for example, if one of the SSMEs were to fail.

The maximum SSME power setting for design of the SLWT, however, has been limited to 106% SSME power for abort. The Space Shuttle program has approved a baseline plan to examine the possibility of certifying the Space Shuttle for intact aborts at a 109% SSME power setting. Because the total thrust from two SSMEs at 109% would be significantly lower than from three engines at 106% power, NASA is encouraged to complete its review of SLWT design limits and raise them to the highest test-verified power level compatible with the flight rules for abort.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Ref: Finding #8

The RSRM manufacturer, Thiokol, expends a significant forward-looking effort in dealing with issues such as obsolescence, environmental constraints, and loss of suppliers. These factors, however, are frequently not under Thiokol's control. Reasonable projections of obsolescence can become difficult because of the large number of tier and subtier suppliers for whom business conditions and regulations can change at any time. A key element of verification for many of the necessary changes is to qualify the change in a Flight Support Motor (FSM) static test motor firing prior to incorporating it into flight production. It is necessary to have an FSM schedule that always ensures a timely static test opportunity. NASA has recently reverted from its planned 12-month FSM firing interval to tests at 18-month intervals. The current rate of changes points to the need for FSM motor firings every 12 months.

LOGISTICS

Ref: Finding #9

NASA continues its laudable efforts to bring "in house" the repair and overhaul of components that the original equipment manufacturer will no longer agree to perform. The time required for these activities is still excessive and needs to be continuously reexamined in an attempt to reduce flow times and, hence, increase spares availability. Currently, the repair processes have considerable "dead" time due to delays in starting failure analysis of removed units. Total repair turnaround time could be significantly shortened if these delays were eliminated. Obsolescence, loss of suppliers, ecological demands, and economic pressures exacerbate this situation.

NASA continues to use Line Replaceable Units (LRUs) removed from the orbiter undergoing an Orbiter Maintenance and Down Period (OMDP) overhaul to support the operating fleet. There is nothing wrong with such efforts if the LRU must be removed anyway as part of the OMDP. However, any unplanned removal of components increases the risk of improper re-installation or damage.

Although there are no approved plans to increase Space Shuttle flight rates, it should be noted that the current level of spares might not be capable of supporting increased flight rates without significant changes in the repair processes or increases in spares inventory.

Ref: Finding #10

The synergy that was developing last year under the USA banner among logistics personnel from the principal contractors, notably Lockheed-Martin and Boeing North American, has apparently blossomed and is encouraging some new thinking with respect to control systems, performance measurement, and personnel efficiencies. The watchword appears to be "what is good for the logistics system?" rather than slavishly following the previous contractual practices. The enthusiastic reexamination and, in some cases, realignment of systems, which may have stagnated from the early 1980's when they were installed and implemented, is yielding excellent results.

An example of this kind of development is a detailed study of a replacement system to the now outdated Kennedy Inventory Management System (KIMS). The replacement utilizes a commercial off-the-shelf system and will be completed around August 1998. The old KIMS will be gradually phased out, terminating entirely by the millennium.

Another good example of system modernization and cost-effective streamlining is contained in the Boeing-Rocketdyne SSME logistics approach. The SSME Component Optimization Program (COP) consists of a model initially "sized" for some 200 LRUs and analyzes asset requirements, abnormal usage spikes, and varying demand scenarios. These data are used as working tools by the spares analysts, and initial indications show that significant time savings and increased confidence levels

are being obtained by use of the system. An evaluation of the payback being afforded by the COP system will be made early in 1998.

Ref: Finding #11

The general characteristics of the logistics and support programs are well controlled in all of the principal contractor programs and show "green" on the green-amber-red scales. Nevertheless, there is enough concern in a few cases to warrant more specific corrective action. For example, obsolescence-induced difficulties with high value and longer lead-time procurement items of electronics (e.g., the Inertial Measurement Unit and the Master Events Controller) require decisive action. Similarly, a number of mechanical components, such as the Freon disconnect and the two-way solenoid valve necessitate urgent attention.

The NASA Shuttle Logistics Depot operated by USA at Cape Canaveral is providing an essential and generally satisfactory component repair and rebuild service. Its limited capability and capacity, however, are resulting in some instances from a growing backlog and consequently increased repair turnaround times. Such issues demand intensive tracking and followup by NASA and USA to avoid downstream crises.

B. INTERNATIONAL SPACE STATION (ISS) PROGRAM

Ref: Finding #12

The manufacturing and assembly process for the ISS is a success-dependent program. Every element must be complete and thoroughly tested prior to launch to orbit. With few exceptions, the modules of the ISS will only be tested as a combined entity after assembly in orbit. This is a challenging task, with associated safety and programmatic risks.

Node #1 was shipped from Boeing at Marshall Space Flight Center to KSC in an unfinished state. There exist current plans to ship other units prior to completion of some component qualification tests. If schedules require, future modules may even be shipped to KSC before completion of assembly. Whatever the reasons for these actions, such practices can open the door to potential mistakes or errors of omission. Something can slip through the cracks and only be discovered on orbit during or after assembly. NASA should ensure that any ISS assemblies that are shipped before completion of the manufacturing, testing, and certification processes are carefully scrutinized to make sure that no safety-related steps are subverted.

Ref: Finding #13

From a safety point of view, it is clear that the Shuttle-Mir (ISS Phase 1) program has been a success. The well-publicized operational problems of the last year have diverted attention from the reality that this multicultural, multilingual team has worked together very well. Complex joint U.S.-Russian activities have been worked out in near-real time, demonstrating the ability to continue to innovate and to accomplish heavy workloads even under high-stress conditions.

The ISS team is focusing on the lessons to be learned from these activities as well as from Skylab and is beginning to develop standard procedures to handle similar circumstances on the ISS. The collision with the Progress module, the several oxygen generator problems, and the multiple computer failures have all served as strong indicators that, for safe operations, it is imperative to plan ahead and provide and train on well-thought-out emergency procedures. It is also prudent to anticipate the need for spare parts/assemblies and prepare for contingencies by storing on board a sufficient stock of critical items for operational repairs.

While the ISS design differs from Mir in many respects, much can be learned by using the Mir experience to develop failure scenarios related to the ISS. These can then be assessed to determine whether the ISS system is capable of handling the posited problems or situations at least as well as was proved on Mir. In order to best undertake these analyses, a multidisciplinary team comprising systems design, operational, and human factors expertise should be formed.

Ref: Finding #14

The 1-year Department of Energy limits for radiation exposure for "radiation workers" are:

300 REM to the skin

50 REM to the blood-forming organs

Extended deployments by astronauts in ISS could result in radiation exposures that exceed those limits. Radiation exposure is cumulative over a lifetime. Design features of the ISS to minimize crew exposure to ionizing radiation are unknown. The dangers of exposure to ionizing radiation should be confronted now with conservative module, system, and equipment designs that minimize exposure. Otherwise, crew stay time may have to be limited.

Ref: Finding #15

One of the more safety-critical subsystems in the ISS is the Caution and Warning (C&W) system. The ISS C&W system is far more complex than previous alarm-only systems in that it will incorporate sensors, processors, displays, communications, and data distribution subsystems and have the ability to conduct certain recovery actions from remote locations. Yet, for a variety of reasons, the system remains immature. The draft *Caution and Warning System Description Document* states that: "The ISS C&W system is designed to inform and assist the onboard crew in resolving and responding to hazardous conditions, or situations that may endanger ISS resources, the lives of the crew, or mission success." To date, the primary focus has been on annunciation of hazardous conditions. The Panel remains concerned that the application of a systems engineering approach to C&W is lagging.

C. COMPUTER HARDWARE/SOFTWARE

Ref: Finding #16

NASA is well aware of the ISS software schedule risk. It has been noted by all levels of management. Considerable effort has been expended to try to resolve this problem. Fifty additional experienced people have been added by the contractor to support the software effort. There are meetings at least every 2 weeks to work on software schedule problems. Thirty million dollars has been allocated to create an ISS System Integration Lab (ISIL) to assist the integrated testing of hardware and software.

Nevertheless, NASA has not found the solution to the software schedule problem. Software specialists believe they have absolutely zero margin, and they see ISS assembly flight 5A as a major hurdle. Some of the software schedule charts reviewed called for software being needed (and delivered) before it was scheduled to be completed.

Even though there is great schedule pressure, no one told the Panel that they felt that they are or would be pressured into sacrificing safety for schedule. However, this always remains a concern.

Ref: Finding #17

NASA has placed emphasis on using Commercial Off-The-Shelf (COTS) software for the Space Station. There is a quandary that results from adopting that decision as opposed to developing specific, unique software. COTS products change frequently, both in response to market needs and to increased hardware capabilities (currently arriving on the scene at least once a year). That creates a major problem for long-lived systems such as the ISS. The COTS software vendors are highly unlikely to maintain their systems for today's (or yesterday's) computers for time periods on the order of decades. They will upgrade their systems for the then-current hardware. After a relatively short time, NASA may lose support for its software development tools.

NASA faces multiple problems from this situation. First, as inevitable errors in the development tools are found, NASA must address the question of repairing them or developing workarounds. Even if NASA "freezes" the versions of the COTS tools being used and uses workarounds for problems that result, there is a larger problem looming related to computer hardware upgrades. Eventually, NASA will have to upgrade the computer platforms supporting the ISS. When that happens, it will be necessary to utilize the tools to regenerate the software for the new platforms. However, the tools themselves will first have to be retargeted to the new platforms. Two problems arise with this. In some cases, there will be no COTS upgrades to the new platforms. In others, the COTS product will have evolved considerably, and major recertification would be necessary.

NASA must be prepared to assume some level of responsibility for maintaining the software tools that it is using, even though they are COTS products. It faces a number of complex decisions in maintaining its COTS tools. NASA must choose between different versions of compilers and code generators and even different versions of the language being used. Of particular concern is the maintenance of the Ada compiler. No Ada compiler vendor has produced a high-quality compiler until at least their second- or (more usually) third-generation product. These compilers are extremely complex, and it seems likely that there will be problems in maintaining them. Consideration of moving to Ada 95 would seem an alternative worth considering.

No simple inexpensive solution is known. It is important, however, that this problem be addressed now, before the problems become a reality, as some of the potential solution alternatives could no longer be available in the future if the problem is deferred.

Ref: Finding #18

NASA's decision to use Intel 80386-based processors for the space station was made in the mid-1980s, more than 10 years ago. While the 80386 was a good choice at the time and had a long service life, today's products are now two or three generations beyond the 80386. The key issues are not solely, or even principally, hardware performance. Rather, it is a matter that NASA is rapidly headed toward operating its COTS products in a world devoid of any other users, as described in the discussion of the previous finding. Moreover, component replacement problems will eventually become an issue. As the Space Shuttle has also shown, there is a never-ending need for upgraded hardware capabilities to increase safety and to take advantage of new technical developments in other areas.

Given the present problem of long-term maintenance of tools and that eventually it will be necessary to upgrade the computer hardware on the ISS, there is likely an advantage to beginning consideration of an upgrade at this time. Some of the solution alternatives to the long-term tool maintenance problem described in the previous finding might be more attractive if it were known that a hardware upgrade was also being scheduled (e.g., whether or not to change the language being used to Ada 95).

The Panel recognizes that it could be difficult to work on this problem now because of the severe schedule problem presently being experienced. However, it is an important problem that will only become larger with time. Its consideration should not be deferred. A small team should be able to develop appropriate upgrade strategies.

Ref: Finding #19

The Checkout and Launch Control System (CLCS) development program appears to be proceeding well. The program includes a massive software effort, with conservative code size estimates of 3 million lines of source code. Therefore, CLCS needs a

strong Independent Verification and Validation (IV&V) activity. Unfortunately, the CLCS program has not been provided with funding earmarked for IV&V.

While a substantial part of the code to be written is an adaptation of existing code, there is little in the way of documentation or requirements for the existing systems. An important activity, then, is to generate requirements and documentation for CLCS. The code development is proceeding in parallel with the development of these requirements and documentation.

The CLCS code is being developed in a series of releases, approximately one every 6 months. This makes the progress of the project visible and provides an opportunity for feedback and revision of requirements at reasonable points in the project. The CLCS incremental development approach can be a very useful method for developing complex software. It can, however, also complicate IV&V activities, necessitating an assessment at each stage of the development.

The development team that has been assembled to work on the CLCS project appears to be very strong. Nevertheless, given the scale of the project and its safety-critical nature, incorporation of adequate IV&V is essential. It is also essential that the quality of the software development not be compromised to fund IV&V, as this would be counterproductive.

D. PERSONNEL

During 1997, the Panel made a point of assessing the employment situation and outlook at each of the NASA Centers visited. Special attention was paid to the situation at KSC, JSC, and MSFC—those Centers most directly associated with the development and operation of the Space Shuttle and the International Space Station. This concern reflected the unanimous view of the Panel that NASA should not permit short-term budgetary pressures to erode the critical competencies that will be required to maintain this country's leadership in space in the 21st century.

The continuing authority to offer a limited "buyout" of NASA employees in exchange for a voluntary resignation, coupled with normal attrition rates, has been sufficient, so far, to avoid a highly destructive involuntary Reduction-in-Force (RIF). Due, in part, to the broader range of technical job skills that exist, JSC and MSFC have been able to manage their declining workforce in a way that has retained younger employees and avoided any serious gaps in job skills and experience. KSC has found it more difficult to manage its workforce in a proactive way: its downsizing target is proportionately larger than JSC and MSFC, and fewer opportunities exist to shift employees into alternative jobs. The potential for shortfalls in key competencies clearly exists.

This potential is exacerbated by the continuing freeze on new hires. Although it is theoretically possible for a NASA Center to receive authority to fill a documented critical skills shortage, the Panel has found that this authority is rarely exercised. Moreover, the job freeze has all but killed a normal pattern of bringing "new blood" into the Agency to replace those who are leaving through retirements, attrition, or voluntary resignations. Where it has been established practice to hire a dozen or so co-op students, along with outstanding "fresh-out" engineering graduates, NASA Centers currently find these traditional channels of identifying the next generation of leadership all but closed. Although these losses are not likely to be noticed in the near term, they clearly place in jeopardy U.S. leadership in space 10 or 20 years from now.

An arbitrary job freeze is an abdication of management responsibility. Given the budgetary constraints that have been imposed by Congress, it makes more sense to provide NASA Centers maximum flexibility to manage people proactively within identified budget levels rather than focus on arbitrary personnel ceilings. Such an approach is fully consistent with the philosophy of NASA Headquarters delegating to the Centers both program responsibility and program authority. Initiatives such as partnering with other Centers, increased use of postdocs/interns/students, limited hiring of fresh-outs, co-ops, and specialized skills, training and cross-training, and targeted buyouts can avoid skills and experience shortfalls while also ensuring the recruitment of NASA's next generation of leaders.

In addition, the management of NASA and USA should recognize the significant shift that has taken place during the past several years within the job market for well-

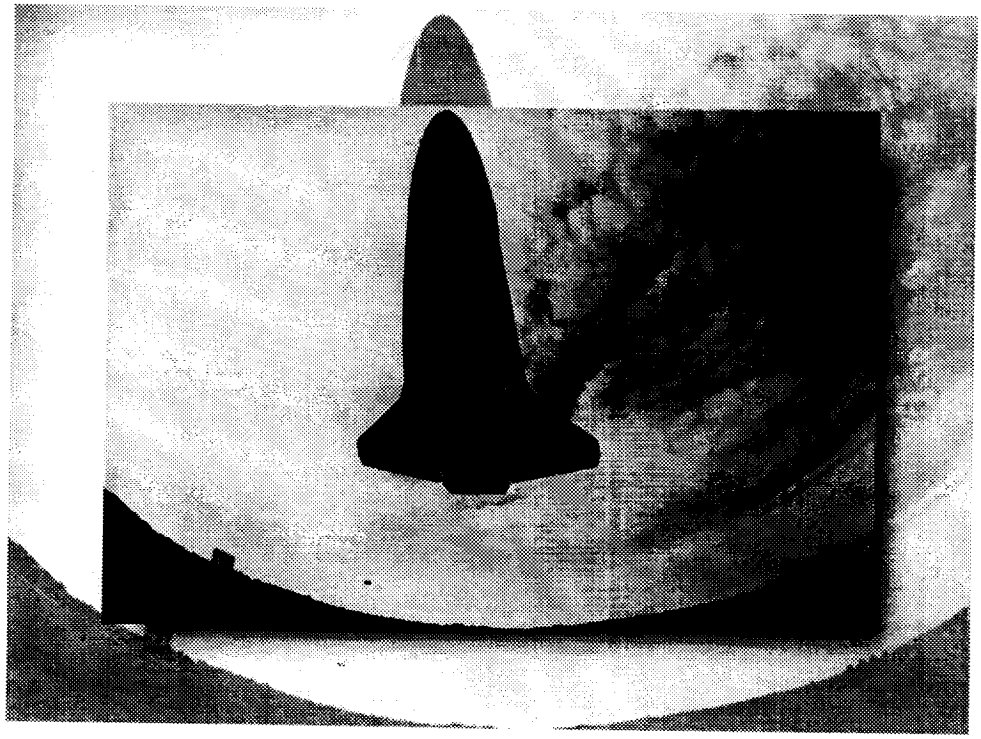
trained engineers. Private sector employers report hiring shortages in key engineering disciplines. Competition for top graduates is intense. NASA and USA must respond positively to this competition if the Nation's space program is to retain its reputation as a place for the "best and the brightest" among the current generation of engineers.

MSFC and JSC have established a proactive skills census that is a useful tool in forecasting skills deficits so that remedial action can be initiated before a shortfall exists. Other initiatives, such as Marshall's EDTec Center and the computer-based Professional Development Initiative (PDI), are examples of innovative training tools being developed to help maintain NASA's technical competencies.

Obtaining ISO 9000 certification can be a valuable exercise in introspection that can lead to a better understanding of an organization's processes and, hence, a higher quality product. To obtain ISO 9000 certification, an enterprise must meet certain rigid standards for documenting and understanding its operations. It must then defend its approaches and documentation as part of an independent examination.

NASA has set a goal for each of its enterprises of achieving ISO 9000 certification within a reasonable period of time. The process of becoming certified, however, does require a considerable amount of staff time. This time was not considered as part of the Zero Base Review, and therefore personnel for this task were not included in Center budgets. Without sufficient staffing, ISO 9000 certification activities have the potential to intrude upon the normal work of NASA Centers, particularly when the workload is already high. To avoid compromising the very quality that ISO 9000 certification is intended to enhance, NASA should adjust certification schedules, if necessary, to permit more time for the process at those Centers that are already heavily loaded.

IV. Appendices



Appendix A

AEROSPACE SAFETY ADVISORY PANEL MEMBERSHIP

CHAIRMAN

MR. PAUL M. JOHNSTONE
Aerospace Consultant
Former Senior Vice President
Operations Services
Eastern Airlines, Inc.

DEPUTY CHAIRMAN

MR. RICHARD D. BLOMBERG
President
Dunlap and Associates, Inc.

MEMBERS

MS. YVONNE C. BRILL
Aerospace Consultant
Former Space Segment Engineer
INMARSAT

VADM ROBERT F. DUNN,
USN (RET.)
Aerospace Consultant/Author
Former Deputy Chief of
Naval Operations Air Warfare
Pentagon

MR. KENNETH G. ENGLAR
Aerospace Consultant
Former Chief Engineer
Delta Launch Vehicle
McDonnell Douglas Corporation

DR. GEORGE J. GLEGHORN
Aerospace Consultant
Former Vice President
and Chief Engineer
Space & Technology Group
TRW, Inc.

DR. SEYMOUR C. HIMMEL
Aerospace Consultant
Former Associate Director
NASA Lewis Research Center

DR. NORRIS J. KRONE
President
University Research Foundation

DR. RICHARD A. VOLZ
Royce E. Wisenbaker Professor
of Engineering
Former Head
Department of Computer Science
Texas A&M University

CONSULTANTS

MR. CHARLES J. DONLAN
Aerospace Consultant
Former Deputy Director
NASA Langley Research Center

VADM BERNARD M. KAUDERER
USN (RET.)
Aerospace Consultant
Former Commander Submarine Forces
U.S. Atlantic Fleet

MR. JOHN F. MCDONALD
Aerospace Consultant
Former Vice President
Technical Services
TigerAir, Inc.

MR. NORMAN R. PARMET
Aerospace Consultant
Former Vice President, Engineering
Trans World Airlines

MR. ROGER D. SCHAUFELE
Professor, Aircraft Design
California State University

DR. JOHN G. STEWART
Partner
Stewart, Wright & Associates, LLC

EX-OFFICIO MEMBER

MR. FREDERICK D. GREGORY
Associate Administrator for
Safety and Mission Assurance
NASA Headquarters

STAFF

MR. NORMAN B. STARKEY
Executive Director
NASA Headquarters

MS. SUSAN M. SMITH
Staff Assistant
NASA Headquarters

MS. CATRINA L. MASON
Secretary
NASA Headquarters

Appendix B

NASA RESPONSE TO FEBRUARY 1997 ANNUAL REPORT

SUMMARY

NASA responded on August 11, 1997, to the "Findings and Recommendations" from the February 1997 Annual Report. NASA's response to each report item is categorized by the Panel as "open, continuing, or closed." Open items are those on which the Panel differs with the NASA response in one or more respects. They are typically addressed by a new finding, recommendation, or observation in this report. Continuing items involve concerns that are an inherent part of NASA operations or have not progressed sufficiently to permit a final determination by the Panel. These will remain a focus of the Panel's activities during 1998. Items considered answered adequately are deemed closed.

Based on the Panel's review of the NASA response and the information gathered during the 1997 period, the status of the recommendations made in the 1997 report is presented on the following page.

RECOMMENDATION

No.	Subject	Status
1	Consequences of Space Flight Operations Contract (SFOC) implementation	Continuing
2	Training and experience of Space Shuttle supervisory personnel post-SFOC implementation	Continuing
3	Measurement of impact of downsizing on the safety of Space Shuttle operations	Continuing
4	Integrity of Space Shuttle processing quality assurance procedures	Closed
5	Operational upgrades to hardware, software, and logistics support for Space Shuttle flight until at least 2010	Continuing
6	Orbiter Reaction Control System (RCS) thruster valve in-flight leaks	Continuing
7	Certification of a new gas generator valve module for the Improved Auxiliary Power Unit (IAPU)	Continuing
8	Future avionics software upgrades	Closed
9	Implementation of the Multi-Function Electronic Display System (MEDS) in the orbiter	Closed
10	Alternate Turbopump Program High Pressure Fuel Turbopump (ATP HPFTP)	Closed
11	Block II schedule	Closed
12	Block II cumulative test time at 109% power level	Open
13	Application of side loads in Reusable Solid Rocket Motor (RSRM) Flight Support Motor (FSM) firings	Closed
14	Flight Support Motor firing schedule	Closed
15	Use of asbestos in Reusable Solid Rocket Motor (RSRM) manufacture	Closed
16	Testing of the 2195 material and quality control procedures used in the manufacture of each Super Light Weight Tank (SLWT)	Closed
17	Transition of logistics functions under Phase I of the Space Flight Operations Contract (SFOC)	Closed
18	Increasing cannibalization rates, component repair turnaround times, and loss of repair capability for the Space Shuttle	Continuing
19	Space Shuttle component obsolescence	Continuing
20	International Space Station (ISS) schedules	Continuing
21	Meteoroid and orbital debris (M/OD) mitigation	Continuing
22	Deficiency of collision avoidance and maneuver process	Open
23	Development of Caution and Warning (C&W) System	Continuing
24	ISS toxic detection and annunciation	Continuing
25	ISS wireless communication system	Closed
26	Development of an ISS Crew Return Vehicle (CRV)	Closed
27	Software safety policy	Continuing
28	Software assurance program roles and responsibilities	Open
29	Use of Matrix X for ISS software	Continuing
30	Documentation of firmware placed in ISS components	Closed
31	ISS software development process	Closed
32	Consolidation of NASA flight research aircraft at Dryden Flight Research Center (DFRC)	Closed
33	Implementation of a wind tunnel inspection plan	Closed
34	NASA's aeronautics research program	Closed
35	Space Shuttle obsolescence	Closed
36	Firefighting preparedness and training	Closed

National Aeronautics and
Space Administration
Office of the Administrator
Washington, DC 20546-0001

AUG 11 1997

Mr. Paul M. Johnstone
Chairman, Aerospace Safety Advisory Panel
24181 Old House Cove Road
St. Michaels, MD 21663

Dear Mr. Johnstone:

In accordance with your introductory letter dated February 1997 to the Aerospace Safety Advisory Panel (ASAP) Annual Report, enclosed is NASA's detailed response to Section II, "Findings and Recommendations."

The ASAP's efforts in assisting NASA to maintain the highest possible safety standards are commendable. Your recommendations are highly regarded and continue to play an important role in risk reduction in NASA programs.

We thank you and your Panel members for your valuable contributions. ASAP recommendations receive the full attention of NASA senior management. In particular, I expect that NASA's Office of Safety and Mission Assurance will track resolution of these issues as part of their role in independent assessment.

We welcome the continuance of this beneficial working relationship with the Panel.

Sincerely,

Daniel S. Goldin
Administrator

Enclosure

1997 AEROSPACE SAFETY ADVISORY PANEL REPORT

Findings, Recommendations, and Responses

A. SPACE SHUTTLE PROGRAM

OPERATIONS/PROCESSING

Finding #1

One consequence of the implementation of the Space Flight Operations Contract (SFOC) is a reduction in opportunities for NASA personnel to maintain detailed, day-to-day work floor interfaces with their contractor counterparts both at space flight centers and major contractor facilities. This could compromise NASA's ability to carry out its assessment function.

Recommendation #1

In order to carry out its assessment role, NASA must maintain some physical presence on the work floor at the space flight centers and major contractor facilities. NASA must ensure that the people staffing these surveillance positions are and continue to be appropriately skilled, thoroughly knowledgeable about the Space Shuttle, and sufficiently experienced with both the subsystem they oversee and the total Space Shuttle system.

NASA Response to Recommendation #1

NASA concurs with the finding and is sensitive to the need to maintain a skilled and capable workforce in both the management and technical functions necessary for Space Shuttle program (SSP) success, and the Agency will work with the contractor in establishing the eventual organizational roles and responsibilities to assure that success. The transition process will be managed at a pace to ensure that necessary skills are maintained within the Government/contractor workforce.

The assessment function that NASA will perform in the future Shuttle operations architecture will require the maintenance of a solid skill base within the Agency. NASA will retain the capability to review all anomalies in operations and system performance, as well as all changes to operations and to systems. NASA's role in requirements control will also provide continuous exposure to designs and operations within the program. The participation of NASA engineering and management in the development of Shuttle upgrades will provide further opportunity for the maintenance of an inherent skill base. Finally, there will be functional roles for NASA personnel, such as astronauts, flight controllers, and mission directors, that will provide an avenue for skills development and maintenance.

Finding #2

It is not clear how NASA Space Shuttle supervisory personnel will be trained and acquire the experience levels necessary to function effectively in senior management positions when the SFOC is fully implemented and the traditional learning ladder positions are staffed by the contractor.

Recommendation #2

NASA should develop and promulgate training and career paths leading to preparation and qualification as potential senior NASA Space Shuttle management.

NASA Response to Recommendation #2

NASA has an active commitment to the development of the skills of senior managers for all functional areas of the Agency. Space Shuttle program senior managers are generally products of both their in-line experiences as well as the NASA career development programs. It is anticipated at this time that the roles for NASA personnel and the career development programs that have served NASA well to this point will be sufficient to assure a continuation of highly qualified and capable senior managers in the future. Given the evolving nature of the NASA and prime contractor roles and responsibilities for the SFOC operational model, it is reasonable to focus special attention on this issue; the program will ensure that specific consideration is given to management development in the transition plans being developed and implemented across the program.

Finding #3

No objective measure has yet been developed, or is likely possible, that can shed significant light on the impact of downsizing on the safety of Space Shuttle operations.

Recommendation #3

In the absence of a valid predictive safety metric, NASA should ensure that all functions affected by downsizing and necessary for safe operations are assigned to people who have the knowledge, skills, and time to carry them out.

NASA Response to Recommendation #3

NASA concurs; all of the contractors supporting the Space Shuttle program remain committed to assuring that safety is the highest priority in every facet of the program. The program recognizes the concerns that downsizing may raise, and it will assure that knowledgeable and skilled individuals are assigned to all critical Shuttle functions, including those being downsized. The plans for the transition of processes and tasks under the SFOC specifically address the safety implications of the transition. As an added assurance, the Shuttle program has required that the NASA Safety and Mission Assurance (SMA) organizations review and concur on the transition plans. Other program downsizing efforts have a similar emphasis on safety embedded in them, and both program management and the SMA management are committed to assure that this focus is not compromised.

Finding #4

Postflight discovery of a wrench and an equipment name plate in the forward skirt of one STS-79 Solid Rocket Booster (SRB) has heightened concern for the overall integrity of Space Shuttle processing quality assurance procedures.

Recommendation #4

NASA, in concert with the several Space Shuttle contractors, should conduct an in-depth review of Space Shuttle processing quality assurance procedures focused on creating a more formal, documented approach to accounting for tools and other material introduced to and removed from flight hardware work areas.

NASA Response to Recommendation #4

The Space Shuttle program element contractors presented their tool control programs to the Space Shuttle System Safety Review Panel (SSRP) meeting in December 1996. The SSRP reviewed the tool control programs of all the contractors and determined that each of the tool programs was effective for the type of work performed. The SSRP recommended that tool accounting audits be maintained or increased, and that metrics be maintained to assure that each tool control program remains effective. In a letter dated March 20, 1997, the Space Shuttle Systems Integration Office confirmed that NSTS 07700, "Space Shuttle Program Definition and Requirements," requires tool control for only the launch and landing project, and recommended that Volume XI of NSTS 0770 be expanded to include tool control at the manufacturing facilities. A change request to NSTS 07700, Volume XI, adding the program requirement to include tool control at the element manufacturing facilities, was approved by the Program Requirements Control Board (PRCB) on July 10, 1997.

Finding #5

NASA plans to operate the Space Shuttle until at least 2012. This will require safety and operational upgrades to hardware, software, and logistics support.

Recommendation #5

NASA should complete Space Shuttle upgrades as soon as possible to take advantage of opportunities for earliest risk reduction and operational improvement.

NASA Response to Recommendation #5

The SSP upgrade strategy is founded on the premise that safety, reliability, and supportability improvements must be made to support human space transportation until a suitable replacement is available. To manage and focus these efforts more effectively, the SSP established the Office of SSP Development on January 16, 1997.

The Space Shuttle upgrades program is being implemented from a systems perspective. Upgrades will be integrated and prioritized across all flight and ground systems, ensuring that individual upgrades are compatible and that their impact is assessed across the entire program.

A phased approach to the SSP upgrades is already under way. Phase I, to be completed by the year 2000, emphasizes safety and performance enhancements for the International Space Station (ISS) assembly and utilization. Ongoing efforts within all SSP elements are also under way to identify Phase II candidate and Phase III/IV studies. Primary emphasis remains on safety and risk reduction by improving reliability and maintainability, eliminating obsolescent components, and improving vehicle performance. As those upgrade candidates are identified by the program elements, the SSP is committed to expediting implementation to maximize safety and reduce overall program risk.

ORBITER

Finding #6

The orbiter Reaction Control System (RCS) thruster valves continue to leak in flight. NASA has aggressively attacked this problem with some success. Procedural changes have improved thruster reliability, and the incidence of leakage has been reduced but not eliminated.

Recommendation #6

Continued attention must be focused on the elimination of the root causes of RCS valve leakage/failures.

NASA Response to Recommendation #6

Several remedial actions have been and are being implemented as a result of a 1995 tiger team investigation into the causes of RCS valve leakage/failure. This has resulted in many procedural changes and several potential hardware improvement concepts. The procedural changes are reducing the number of in-flight thruster valve failures. Many of the hardware improvements are entering a development testing phase. Examples of procedure and hardware changes include:

- Preventative maintenance flushing. Water flushing of the RCS pilot operated valves (POV) was developed at the White Sands Test Facility (WSTF) and has been verified to remove iron nitrate contamination from the POV.
- Manifold thruster preventative change-outs. It is now required to change all thrusters on a manifold when that manifold is drained for any reason. The removed thrusters are sent to WSTF for water flushing and then returned to spares.
- Hard-filled manifold processing. The POV has demonstrated substantially better sealing capability in a fully wetted, hard-filled condition. KSC procedures have been implemented that provide the ability to maintain a hard-filled manifold configuration when performing work on the RCS pods.
- Minimization of moisture intrusion. Several additional recommendations have been implemented that specifically address minimizing moisture intrusion into the propellant system.
- Redesigned POV (RPOV). Another result of the critical examination of the RCS POV failure history was the recommendation that the oxidizer POV be redesigned to improve the ability to withstand nitrate contamination. The resulting RPOV is proceeding through buildup and development testing. The RPOV design addresses the areas in the current valve that are known to be sensitive to nitrate contamination.
- Minimization of oxidizer moisture and iron content. The presence of iron and water in nitrogen tetroxide greatly increases the potential for precipitation of iron nitrate

internal to the POV pilot cavity. Therefore, a molecular sieve is being designed and fabricated to reduce the levels of iron and water in nitrogen tetroxide.

Finding #7

A new gas generator valve module for the Improved Auxiliary Power Unit (IAPU) is currently entering the process of certification. When fully certified, the IAPU with this new valve is planned to be qualified for 75 hours of operation between scheduled teardowns and overhauls (in excess of 10 years at projected use rates).

Recommendation #7

Once certification is achieved for 75 hours of IAPU operation, NASA should establish a periodic inspection and test program to assure that IAPUs continue to perform in accordance with requirements throughout their service life.

NASA Response to Recommendation #7

An IAPU maintenance plan is being developed by the NASA and contractor technical community. Current activity is focused on developing a maintenance specification, evaluating long-term life of elastomeric components, and organizing a parts tracking/usage database. At the conclusion of this effort in late FY 1997, a long-term maintenance plan will be baselined for implementation. Supplementing this to provide long-term service life information is a fleet leader test program at WSTF. The WSTF program is currently scheduled to conclude in FY 1999 and is to demonstrate 75-hour run time and evaluate 10+ year teardown and overhaul time.

Finding #8

The Space Shuttle is about to receive two major avionics upgrades—a triple redundant Global Positioning System (GPS) installation and the Multi-Function Electronic Display System (MEDS)—both of which require significant changes to the Primary Flight Software (PFS) and Backup Flight Software (BFS) systems.

Recommendation #8

The Space Shuttle program should ensure that both the GPS and MEDS software changes are thoroughly tested in the Shuttle Avionics Integration Laboratory (SAIL) using the normal and enhanced test protocols that have proved to be robust when testing major modifications.

NASA Response to Recommendation #8

The SSP concurs that all software and hardware changes need thorough testing, and it recognizes the extremely important role that SAIL testing fulfills in the complement of testing for software certification. All Shuttle software or hardware upgrades are assessed to determine integrated verification test requirements. The SSP and its contractors cooperate to produce integrated hardware and software test implementation plans, test requirements documents, and integrated test schedules to assure that the required resources, including SAIL, are available. All these plans are reviewed and approved by the program. Thorough testing of each new capability is

then performed and analyzed. This same rigorous process that is used for flight software Operational Increment (OI) updates will be applied to the MEDS, GPS, other Shuttle upgrades, and future software updates.

Finding #9

The Multi-Function Electronic Display System (MEDS) in the orbiter is being implemented with display functions and formats that mimic the present electromechanical and cathode ray tube presentations. There are significant potential safety and operational benefits from enhancing the amount, type, and format of information shown on the MEDS displays.

Recommendation #9

The Space Shuttle program should commit to a significantly enhanced MEDS display as soon as possible. The MEDS advanced display working group or a similar multidisciplinary team should be tasked with identifying specific modifications and an associated timetable so that the opportunities inherent in MEDS can be realized.

NASA Response to Recommendation #9

The SSP has established an enhanced MEDS program that includes hardware and software enhancements to take full advantage of MEDS capabilities. This includes hardware expansion as well as utilization of inherent MEDS capabilities to provide better displays and improve crew situational awareness. Additionally, an SSP Cockpit Upgrade Team is being formed to develop advanced display and application concepts for future implementation into MEDS/enhanced MEDS/future avionics upgrades capability. The Cockpit Upgrade Team will also participate in avionics upgrades discussions in order to anticipate future hardware and software changes and develop advanced cockpit applications to further improve crew awareness and reduce crew training requirements. Initial testing of new applications for enhanced MEDS will begin in June 1997.

SPACE SHUTTLE MAIN ENGINE (SSME)

Finding #10

The Block II SSME development program has proceeded well, except for the Alternate Turbopump Program High Pressure Fuel Turbopump (ATP HPFTP). The HPFTP has suffered significant failures in testing, which were traced to shortcomings in hardware design details. Corrective actions have been implemented on the HPFTP. Block II engine testing has resumed for this major safety improvement.

Recommendation #10

Continue the development and certification test programs as originally planned. Accumulate the specified test operating times for the modified ATP HPFTP, and employ the number of test pumps as per the original test plan.

NASA Response to Recommendation #10

The SSME project is committed to meet the original development and certification plan requirements. The schedule for certification has been adjusted to accommodate comprehensive resolution of the development problems. Scheduled completion of certification testing is now February 1998. As originally planned, the total "hot-fire time" for development and certification will exceed 60,000 seconds, utilizing eight HPFTP units. Certification will be based on two units with 22 tests each, and "hot-fire time" of 11,000 seconds per pump or 22,000 seconds total certification time.

Finding # 11

The schedule for the first flight of the Block II engine has slipped, from September 1997 to December 1997. This schedule is optimistic and contains no slack for future development problems. The schedule also requires continued availability of three test stands at the Stennis Space Center (SSC).

Recommendation #11

Maintain the full scope of the planned test programs. Assure the availability of test stand A-2 at SSC for as long as it is needed for the Block II engine test programs so that three test stands continue to be available.

NASA Response to Recommendation #11

The development and certification test programs will be maintained as originally planned. Test stand availability has been coordinated with other program test requirements to support completion of Block II HPFTP certification testing in February 1998. Three test stands are required only until July 1997 to support this schedule. A mid-May milestone to initiate construction authorization for the July reconfiguration of Test Stand A-1 for X-33 testing will be reassessed based on fuel pump development status at that time. The other two test stands will remain dedicated to SSME testing. After test stand modification, conversion back to SSME test configuration would take approximately 1 month. The first flight of the Block II configuration has been reassigned to STS-91, currently scheduled for May 1998.

Due to the development problems with the ATP HPFTP and the associated schedule slips, the SSP has elected to certify an interim Block II configuration, designated Block IIA. Block IIA will consist of Rocketdyne's current HPFTP in conjunction with the other Block II components and will provide the safety and reliability benefits of the large throat main combustion chamber at the earliest opportunity. This configuration will be certified to fly nominal missions at 104% to 104.5% rated power level (RPL) and will maintain the current 109% RPL contingency abort capability.

Finding #12

The Block II engine will be certified for operation at 109% power level only for abort situations. Accordingly, the test program provides only limited cumulative test time at this thrust level.

Recommendation #12

After completion of the current planned Block II certification test program, conduct a certification extension test program that will demonstrate the highest thrust level for safe continuous operation achievable by the Block II configuration. This program should attempt to achieve at least the 109% power level.

NASA Response to Recommendation #12

The Block II program was developed to "improve the safety, reliability, and robustness of the SSME" by providing lower operating temperatures, pressures, shaft speeds, and other critical parameters. An increase in operating power level from 104% to 104.5% will offset some of the weight gain of Block II. The Block II SSME was never intended to increase Space Shuttle ascent performance or increase payload capability to orbit. However, additional performance has been accepted for a few specific missions at the cost of some of the improved safety margin. There is a commitment that the ISS flights will provide 106% engine power level certification to achieve mandatory critical payloads to orbit. The Block II certification will also provide a 109% intact abort capability, which will allow the vehicle system to better optimize abort scenarios. Implementation recommendations for use of 109% throttle for intact aborts will be made by the Shuttle operations element once certification is complete.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Finding #13

Changes in the Pressure Sensitive Adhesive (PSA) and the cleaning agent for the J-flap of the RSRM were driven by environmental regulations. The certification testing for these changes included a Flight Support Motor (FSM) firing without the application of side loads, a significant condition for RSRM field joints for which the J-flap plays a role.

Recommendation #13

Employ the application of side loads in all future RSRM FSM firings.

NASA Response to Recommendation #13

The SSP and RSRM project agree with this recommendation when aft field joint test objectives warrant inclusion on an FSM test motor. During Space Shuttle return-to-flight RSRM redesign, the assessment of strut loading on the solid rocket motors concluded that the only influence was at the aft field joint. The influence on the aft field joint gap openings was predicted to be less than 0.001 inch, roughly an order of magnitude less than the contribution of the internal motor pressures. Side loads were included on two RSRM static test motors (QM-7 and -8) in a comprehensive effort to include every element of flight loading influencing the aft field joint gap openings. Joint gap openings were not measured directly, but the sealing systems performed as expected. Gap openings were measured on the RSRM structural test article-3, where testing showed side loads influence to be less than 0.0005 inch out of a total of 0.0084 inch for aft field joints only.

The consideration to include side loads on all future tests would not come without technical penalty. To accommodate the side load forces, the aft test stand must be locked out, and as such, no thrust measurements are obtained. Also, no thrust vector control (TVC) duty cycling is performed during the side load events, which requires modification to the baseline static test duty cycle; for certain test objectives, this is an important requirement consideration. This baseline TVC duty cycle is utilized to allow direct performance comparisons between static tests, primarily associated with nozzle and aft dome materials or components. Therefore, a generic inclusion of side loads on all future FSM tests would require elimination of other test considerations, which, depending on specific test objectives, might be a qualification necessity.

In conclusion, the RSRM static test policy includes side loads on full-scale static test motors where there are test objectives associated with the aft field joints, which could be influenced by side loads.

Finding #14

There are many material and process changes in work for the RSRM in response to both environmental regulations and obsolescence issues. A vital part of the certification program for these changes is the demonstration of the acceptability of the

changes during an FSM firing. At present, FSM firings are scheduled at 2-year intervals instead of the 1-year or 18-month intervals previously used.

Recommendation #14
Considering the large number of changes in RSRM materials and processes and the importance of proper simulation of operating conditions in any certification test program, NASA should reevaluate its decision to have 2 years between FSM firings.

NASA Response to Recommendation #14
The RSRM project presented an assessment of static test motor frequency to the PRCB on February 27, 1997, and recommended static tests at 1-year intervals. The recommendation was accepted by the PRCB. An initiative is under way to ensure that the maximum possible benefit is obtained from each test.

Finding #15
A substantial program effort is under way to eliminate the asbestos used in RSRM manufacture and replace it with more environmentally acceptable (i.e., "asbestos-free") materials. Although some of the materials tested to date meet specifications, they do not provide as high structural and thermal margins as the asbestos-containing materials.

Recommendation #15
To maintain flight safety, NASA should not eliminate the use of asbestos in RSRM manufacture. An environmental waiver should be obtained to continue its use in RSRM insulation, liners, inhibitors, and other motor parts in the event of future regulatory threat to the asbestos supplier.

NASA Response to Recommendation #15
NASA currently has no plan to introduce nonasbestos-based replacements for asbestos-based components in RSRM production. The RSRM production and flight history are baselined with asbestos-based materials, primarily NBR rubber. Asbestos is also a constituent of liner and adhesives. The production, handling, and disposal processes for these materials are performed in compliance with strict state, Federal, and local controls and regulations regarding asbestos material. There are no currently identified regulations to ban production or use of asbestos materials in the RSRM supply chain. Because there is no existing or pending regulation, pursuit of waivers or exemptions is not applicable at this time.

NASA considers it prudent to continue low-level development of possible alternative nonasbestos materials. This reflects NASA's sensitivity to the environment, worker safety and health issues, and the fact that the shelf life of these materials precludes the option to stockpile. This development effort is being carried out to provide limited contingency development at a routine pace. The recommendations by both the ASAP and the RSRM initiatives to find alternative materials are consistent with program policy documented in SSP letter MS 96-071, dated September 16, 1996. The policy seeks to balance flight safety and environmental protection goals.

EXTERNAL TANK (ET)

Finding #16

The 2195 aluminum-lithium alloy used in the tank walls and domes of the new Super Light Weight Tank (SLWT) has a lower fracture toughness at cryogenic temperatures than was anticipated in the design. To compensate for this potentially critical shortcoming, NASA has limited the pressure used in the full tank proof test and has recognized that acceptance of each SLWT for flight is highly dependent on far more stringent quality control of the materials and processes used to manufacture the SLWT than is required for the current external tanks.

Recommendation #16a

Assure that the acceptance tests of the 2195 material and the quality control procedures used in the manufacture of each SLWT continue to be sufficiently stringent, clearly specified, conscientiously adhered to, and their use unambiguously documented.

NASA Response to Recommendation #16a

The SSP and Marshall Space Flight Center (MSFC) will continue to ensure that material acceptance testing and the quality control procedures used in the manufacturing of SLWT's are of a sufficient quality to validate that each tank is fully in compliance with all program requirements and is safe to fly.

Recommendation #16b

The criticality of these quality control operations makes it mandatory for NASA to retain buyoff of the results of those fabrication operations and tests that are essential in determining SLWT safety.

NASA Response to Recommendation #16b

The SSP and MSFC will retain NASA approval of the quality control program and changes to that baseline.

Recommendation #16c

As quality control data on the size of flaws detected in 2195 aluminum-lithium material are collected, they should be used in an updated analysis of the SLWT structure, because it may permit the verifiable spread between flight limit stress and proof stress to be raised above that presently reported.

NASA Response to Recommendation #16c

The simulated service database has been developed from data collected on fracture specimens with flaws that are 0.175 inch long. The data verify a 2.9% positive spread between the flight and proof-test conditions. Using the demonstrated flaw detectability level for our nondestructive evaluation dye penetrant process (0.086 inch long) would increase the spread to approximately 14%. Because of uncertainties, it is NASA's standard policy to use a factor of two on our flaw detectability limit. This methodology provides the proper risk allocation between the nondestructive evaluation capability and proof-test levels. The use of a flaw size of 0.175 inch for the simulated service tests is conservative for the SLWT.

LOGISTICS

Finding #17

Transition of logistics functions under Phase 1 of the Space Flight Operations Contract (SFOC) appears to be taking place smoothly. Key personnel are maintaining continuity in management techniques and processes.

Recommendation #17

Continue adherence to established systems, and make maximum use of the inherent capability of the incumbent personnel in the logistics systems.

NASA Response to Recommendation #17

NASA concurs. The established NASA Logistics Operations continues to monitor the established logistics systems and enhance others in order to maintain insight into the logistics activity. Both the SFOC contractor and NASA Logistics Organization have retained incumbent key personnel with critical logistics skills to minimize the transitional risks and continue to support the SSP.

Currently, the SFOC contractor is studying the horizontal consolidation of like functions and processes. NASA Logistics Operations will monitor the contractor's progress to assure that the logistics systems resulting from this consolidation will be capable, effective, efficient, and, above all, not adversely impacting the safety of operations.

Finding #18

Long-term projections suggest increasing cannibalization rates, component repair turnaround times, and loss of repair capability for the Space Shuttle logistics and support programs.

Recommendation #18

Take early remedial action to control this potential situation, such as maintaining sufficient spares and extending repair and overhaul capability.

NASA Response to Recommendation #18

NASA is closely monitoring logistics trends. The areas of emphasis stress long-term logistics support indicators, specifically backlog and repair turnaround. While an increase in repair turnaround time has been noted, vehicle support remains at the same high level. Budget reductions in past years have meant that fewer spares have been produced and less repairs were performed, but NASA and the contractor will continue to manage the process to maintain acceptable levels of support. Presently, logistics performance measurement data do not indicate any adverse trends in cannibalization rates.

NASA has directed SFOC management to maintain an emphasis on logistics supportability during the transition of all contract responsibilities. The SFOC contractor has been directed to maintain key personnel with critical logistics skills to

minimize transitional risks and provide continuity to Shuttle logistics support. In addition, SFOC is required to develop and submit original equipment manufacturer (OEM) contingency plans for responding to known and potential support issues at effected OEMs. All known supportability threats are tracked and evaluated to determine the associated risk and required actions for resolution. The SFOC has the appropriate processes in place to both monitor and respond to loss of subcontractor capability. The NASA Shuttle Logistics Depot (NSLD) has been certified to make some repairs where there has been a loss of critical supplier capability. The SFOC is also considering consolidating similar work at one vendor so that the NSLD is not the only repair agent.

Finding #19

Obsolescence of components and systems on the Space Shuttle is an increasing problem threatening critical spares availability.

Recommendation #19

Alternative components must be developed and certified, and, where necessary, systems must be redesigned to use available or adaptable units.

NASA Response to Recommendation #19

NASA continues to identify and coordinate obsolescence issues concerning hardware, special test equipment, vendor capability, and environmental restrictions with the appropriate design center. Each issue is evaluated for logistics impacts, and this information is communicated to or within the design center so that appropriate action can be taken to initiate any required redesigns, modifications, or enhancements. A Kennedy Space Center (KSC) logistics priority list is maintained to communicate logistics' top concerns to design center management. While obsolescence will continue, a team approach to problem identification, prioritization, and resolution appears to be providing effective problem resolution. Additionally, the Shuttle upgrade program is designed to assure that potential problem areas are addressed so as to preclude disruption in meeting manifest requirements.

B. INTERNATIONAL SPACE STATION (ISS)

Finding #20

The schedules for ISS buildup are tight, and there is little, if any, schedule slack to accommodate late or unavailable hardware. Schedule and/or budget pressures could lead to deferring work to orbit or curtailing prelaunch testing.

Recommendation #20

ISS program plans for finishing and testing hardware before launch should not be compromised to meet either launch schedules or budgets.

NASA Response to Recommendation #20

NASA concurs. Integration testing is in the approved program's current baseline. Prelaunch integrated testing at KSC is based on the degree to which this testing abates program risk, weighed against the hardware damage risk and the cost and schedule impacts. The content for component, subassembly, and element-level testing is the minimum requirement for specification compliance verification. A program-approved change would be required to eliminate this work. In fact, integration and testing are being strengthened as opportunities develop. A proposal to conduct multi-element integration testing is being planned, which would exploit the unique KSC ground processing expertise. This would involve actual flight hardware to conduct end-to-end testing for assembly elements 3A, 4A, 5A, and 6A in the manner that these elements would be assembled on-orbit.

ISS program requirements for on-orbit stage and assembly-complete capability reflect a thoroughly reviewed baseline. This baseline generally reflects a minimum required capability, which has incorporated improvements to satisfy an achievable crew workload. There is strong inherent resistance in the program, therefore, to bringing incomplete hardware to be processed at KSC, much less than to orbit, because of the minimum capability constraints and crew workload impacts.

Finding #21

The overall design philosophy for meteoroid and orbital debris (M/OD) mitigation has been agreed to, in principle, by the international partners. Much of the U.S. module shielding design is nearing completion. Nevertheless, there remains a finite probability that a penetrating collision will occur during the life of the ISS mission. The emphasis of the M/OD effort is therefore shifting to operations issues, such as caution and warning, damage control, and strategies for reaction to depressurization events.

Recommendation #21

Agreement with the international partners should be completed. Operational strategies and procedures for handling M/OD events should be developed and incorporated into ISS plans and schedules. Crew training programs to accommodate these strategies and procedures should be established.

NASA Response to Recommendation #21

The Common Depressurization Strategy (CDS) team was formed in May 1995 to coordinate the program approach for responding to a potential depressurization event. The team's charter is to address crew and vehicle operational strategies, immediately identify required hardware modifications to make safe the vehicle and crew, and develop necessary plans for implementation of these items. Baseline crew procedures, repair requirements, assessment methodologies, and identified hardware modifications (to reduce risks of vehicle and crew loss in the event of a penetration) are documented in international protocol agreements. Plans for implementation are being developed. This approach has been independently reviewed and validated in a series of joint meetings led by Lt. Gen. Thomas P. Stafford (USAF, Ret.) of the NASA Advisory Council and Academician Vladimir F. Utkin of the Russia Space Agency Advisory Expert Council. Specific activities have been agreed to and will be completed by December 1997.

Finding #22

The collision avoidance and maneuver process for evading meteoroids and orbital debris is complicated and not yet completely worked out for many of the scenarios likely to occur during the life of the ISS program.

Recommendation #22

The collision avoidance and maneuver process must be worked out in detail and documented in interagency memoranda and in agreements among the international partners.

NASA Response to Recommendation #22

NASA has a history of cooperation with the U.S. Air Force Space Command (USSPACECOM). Several Memoranda of Agreement (MOAs) are in place with USSPACECOM for Shuttle collision avoidance procedures. The requirements for the ISS are being worked through an established working group. A Debris Avoidance Operations Plan was drafted in 1996. Required international participation is being and has been worked through hardware specifications, international protocol agreements, and the Station Program Implementation Plan. A Flight Mechanics Working Group has been chartered, which includes Russian and NASA participation. This group meets regularly, and their results are documented in the ISSP Flight Rules Manual.

Finding #23

Design of the Caution and Warning (C&W) system had been lagging behind that of other ISS systems. Priority has now been given to the system engineering effort that is required to resolve conflicting operational concepts and to finalize the design.

Recommendation #23

Continue to apply high-level system engineering attention to the expeditious resolution of C&W design philosophies and implementations.

NASA Response to Recommendation #23

NASA concurs. The ISS Caution and Warning (C&W) system has matured throughout 1996, with improvements in tone commonality, event definition, Personal Computer System (PCS) display development, application code generation, and recognition by all program elements. The C&W System Integration Team's (CWSIT) primary purpose is to ensure that the C&W system is safe, robust, and integrated throughout the vehicle and throughout the lifetime of the program. The team's primary responsibilities include:

- Providing end-to-end C&W design integration, including display and response concept definition
- Developing and leading a forum for resolution of C&W design/operational issues

Attachment 1 provides specific responses based on the current design for the examples cited in Section III: Information in Support of Findings and Recommendations, ASAP Annual Report, February 1997.

In addition, in response to the ASAP concerns, the International Space Station Program Office (ISSPO) has tasked two independent assessments of caution and warning activities. These efforts are led by the Manager, ISS Independent Assessment, and the ISS Chief Engineer. These assessments were completed in August 1997.

Finding #24

The ISS has no requirement for sensing a toxic substance spill within a payload rack. The ISS does require that toxic substances in payload racks be multiply contained.

Recommendation #24

The ISS should require payload providers to include, as part of their system design, detection and annunciation of any toxics they carry or could generate.

NASA Response to Recommendation #24

NASA concurs. The approach for payloads on the ISS is patterned after the Shuttle approach. The payload design requirements are defined in NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System," and the ISS Addendum, which to date make the possibility of having a toxic spill so remote as to be an acceptable risk. Requirements imposed on payloads include containment levels stipulated based on level of toxicity of the substance or use of an approved pressure vessel.

The payload provider is required to obtain approval by the Payload Safety Review Panel (PSRP) for the use of any toxic substance, as well as the containment method utilized. Through the safety process defined in NSTS 13830, "Implementation Procedure for STS Payloads System Safety Requirements," all potentially toxic substances are labeled and documented in crew procedures, along with any cleanup

instructions. This ensures that needed information on any potentially toxic substance is readily available to the crew. This concept for the handling of toxic substances is based on Shuttle and Mir program experience and has not been changed.

When payloads are reviewed by the PSRP, compliance with the above requirements must be demonstrated. Astronaut training and procedures are reviewed and approved to ensure that the crew is adequately educated to avoid inadvertently mixing toxic chemicals. In addition, the payload design must still be able to tolerate the appropriate number of operator errors.

These requirements do not impose design solutions on payloads; rather, they require the payload providers to proactively consider their own design solutions to avoid toxic mixing. Enforcing these requirements in the PSRP process by ensuring compliance with the requirements of NSTS 1700.7B will restrict the possibility for toxic mixing to an acceptable risk. Dependent on a case-by-case analysis, the PSRP or the payload provider may request detection and monitoring. The detection will then be provided by the payload provider organization with tie-in to the ISS core systems of C&W (annunciation) provided by core system interfaces at the rack level. This service will then be defined in the appropriate Interface Definition Document (IDD).

The crew will be used to enunciate any toxic spills throughout the ISS. This is considered essentially the equivalent of the panic alarm. The crew will also be used to detect any toxic spill. Studies have shown that intermodule ventilation will spread any toxic gases to all elements of the ISS within 20 minutes, which makes station-level detection not practical.

This further illustrates the importance of having adequate design requirements imposed on payloads to preclude toxic spills. Crew annunciation and detection have been considered acceptable because of the design requirements imposed on the payloads to maintain appropriate levels of containment. However, should a toxic spill occur, provisions are available to payloads for cleanup. These include a crew contamination protection kit (goggles, chemical resistant bags, chemical resistant gloves, emergency eyewash), a portable breathing apparatus, a combustion products analyzer, a volatile organics analyzer, multiple airborne trace contaminant control equipment, vacuum access, and module depressurization. The JSC Mission Operations Directorate is currently developing procedures to respond to a toxic spill. The procedures will be based on Shuttle experience. The response will depend on the hazard level of the substance, the state of the substance (liquid, gas, or solid), the location of the spill, and the size of the spill.

Finding #25

The ISS design does not include a requirement for a wireless communication system to maintain crew contact throughout the station. The present design requires a crew member to translate to a panel or connect a headset.

Recommendation #25

The ISS program should establish a requirement for "hands-free" communications with crew members to deal with situations such as injuries or meteorite/debris impacts in which it may be necessary to establish rapid contact.

NASA Response to Recommendation #25

The requirements specification for this capability has been developed and is provided in Attachment 2. The Station Wireless Communications Subsystem (SWCS) will be installed on orbit no earlier than assembly flight 6a.

Finding #26

The X-38 research vehicle program is a good approach for developing an ISS Crew Return Vehicle (CRV).

Recommendation #26

Any CRV resulting from the X-38 program should be capable of fulfilling the design reference missions that were developed by the Space Station Freedom program for an assured CRV.

NASA Response to Recommendation #26

The ISS program and the X-38 project are developing a top-level set of requirements and dependencies between the ISS and the CRV derived from the X-38. This document, the Performance and Support Requirements Document (PSRD), specifies the three basic CRV design reference missions (return of an injured or ill crew person, emergency evacuation of the station, and return of crew in case the ISS cannot be resupplied) as defined in the top-level Station Specification, SSP 41000. These three design reference missions are the same as used for the ACRV during the Space Station Freedom program.

C. COMPUTER HARDWARE/SOFTWARE

Finding #27

NASA's Agencywide software safety policy allows projects latitude to tailor their software safety plan for safety-critical software. It does not, however, require projects to obtain center Safety and Mission Assurance (S&MA) approval of the tailored software safety plans nor does it require Verification and Validation (V&V) per se. While the software assurance standard does mention V&V, it does not require any independence of V&V for safety-critical software.

Recommendation #27a

NASA should require approval of a project's tailored software safety plan by both the center S&MA organization and by one administrative level higher than that making the request.

NASA Response to Recommendation #27a

NASA agrees with the intent of this recommendation but believes the requirements for formal system safety program plans and software management plans exist and, with proper and firm enforcement, fulfill the objective of this recommendation. To be sure that these requirements are perfectly understood, the Office of Safety and Mission Assurance (OSMA) will update NSS 1740.13, "NASA Software Safety Standard," to explicitly state that the program/project manager for programs/projects perform an assessment to determine, based on the level of criticality and risk, the scope and level of Independent Verification and Validation (IV&V) to be planned. The results of the assessment will be formally reviewed by Center Safety and Mission Assurance (SMA). The program/project manager, in consultation with SMA, will tailor an approach to ensure that the appropriate V&V requirements are established and implemented. The OSMA will place more emphasis on the implementation and enforcement of these existing requirements. Process verification, recently established in the OSMA, will be used to evaluate and enforce these existing policy and requirements more aggressively.

NASA is committed to assuring that required program management plans and any subordinate plans such as software or safety management plans cover the essential requirements for programs where warranted by cost, size, complexity, lifespan, risk, and consequence of failure. Additional changes are being incorporated into NPG 7120.5, "NASA Program/Project Management Guide" (currently under development), to ensure that necessary and sufficient requirements will be fulfilled for programs having software vulnerabilities. SMA organizations at each level are to be a party to these decisions and are to intervene where necessary to assure that proper and clearly documented decisions are made by the appropriate level of management. The Program Management Councils could play a role in adjudicating any issues with the content of program management plans.

Recommendation #27b
NASA's software safety plan should require formal V&V of safety-critical software. Testing alone does not suffice.

NASA Response to Recommendation #27b
NASA agrees with the intent of this recommendation and is confident that NPD 2820, "NASA Software Policies" (currently under development), will ensure that software management and/or safety plans developed for any NASA program/project will specify the level of V&V and types of testing that should be implemented. NPD 2820 policy relating to software V&V states that NASA will create and/or acquire and maintain software through risk-based management. Risk management products shall be documented or referenced in a management plan. NASA will employ V&V, IV&V, and other trusted verification techniques for appropriate risk mitigation based on the cost, size, complexity, lifespan, risk, and consequence of failure. NSS 1740.13 is not a NASA Software Safety Plan. The level of detailed requirements that the ASAP is recommending be in NSS 1740.13 more appropriately belongs in the documents that the programs and projects will prepare in response to NSS 1740.13. These details need to be documented in the Software Management Plan (SMP), the System Safety Program Plan (SSPP), or the Program Management Plan (PMP). NASA maintains that the requirement stated in NASA-STD-2100-91, "Software Documentation Standard," suffices as a requirement for addressing the issue of V&V for programs.

NHB 1700.1, "NASA Safety Policy and Requirements Document," requires NASA program managers to publish and maintain an approved NASA Safety Management Plan (SMP). The program manager is responsible for approval of the NASA SMP and contractor Safety Program Plan (SPP). The system safety manager (SSM), assigned by the program manager (PM) from the Center Safety and Mission Assurance organization, prepares the SMP. The SSM, reviews the contractor's SPP and provides recommendations to the PM. The SSM, upon review of the contractor's SPP, will have the required insight into the approach for software V&V to ensure that a proper balance of analyses, inspections, and testing is planned for the entire life cycle of the program. NASA's SMA organizations at the NASA Centers are currently involved in the review of V&V plans for software and do make recommendations to the PM.

Recommendation #27c
NASA should develop an explicit policy that requires independent V&V for safety-critical software.

NASA Response to Recommendation #27c
NASA agrees with the premise that safety-critical software is a prime candidate for IV&V; however, it is NASA's position that all software determined to be safety-critical by engineering or safety analyses need not be subjected to IV&V. To be sure that program/project managers plan for the proper level of both V&V and IV&V

from the outset, the OSMA will update NSS 1740.13, "NASA Software Safety Standard," to explicitly state that program/project managers perform an assessment to determine the scope and level of IV&V based on the level of criticality and risk. The results of the assessment will be formally reviewed by SMA. This way, the program/project manager, in consultation with SMA, will tailor an approach to ensure that the appropriate V&V requirements are established and implemented. NPD 2820 has incorporated the proper approach for software on NASA programs/projects; the directive requires program managers to employ IV&V, V&V, and other proven verification techniques for risk mitigation, based on cost, complexity, risk, and consequence of failure. NPG 7120.5, "NASA Program/Project Management Guide" (currently under development), will reflect some of the requirements now found in documents that program managers may not normally review for compliance.

Finding #28

NASA has put considerable effort into the reorganization of its software activities and has made significant progress. It does not yet, however, have a comprehensive, clear set of roles and responsibilities for various groups within the Agency with respect to software development, safety, V&V, and software process development.

Recommendation #28

NASA should ensure that there is a clear, universally well-understood, widely promulgated, and enforced NASA Policy Directive on the roles and responsibilities of its various organizations vis-à-vis software development and safety. Moreover, that Policy Directive should specify organizational roles and responsibilities solely on the basis of technical and administrative capability.

NASA Response to Recommendation #28

NASA agrees with the recommendation. The July 1996 (draft) program plan for the Fairmont (IV&V) Facility is the contract between Code Q and the Facility and will be updated for future funding and delegation of the software assurance program. NASA concurs that the draft plan now contains ambiguities but will be clarified in the next update.

The IV&V Facility's reporting structure will be finalized in the upcoming proposed Ames Research Center reorganization. It is anticipated that the IV&V Facility will be moved from under the direction of Code I at Ames and installed as the equivalent of a Directorate in the new ARC organization.

The IV&V Facility Business Plan currently defines the roles and responsibilities of the IV&V Facility. NASA Headquarters will establish and document at the policy level the roles in the Agency for all software, including embedded and flight system software. The policies document will explain how the roles and responsibilities of the Agencywide software efforts mentioned in the finding (e.g., CIO, COE-IT, IV&V Facility) fit together in a synergistic manner within the Agency.

The new NPD 2820 will define Agency policy for program/project utilization of the IV&V Facility. The Chief Information Officer, the Chief Engineer's Office, the Office of Safety and Mission Assurance, and the Software Working Group will be responsible for increasing Agency awareness of all the software-related resources, policies, and existing standards. The newly implemented Code Q process verification activity will validate Agency project managers' awareness of software assurance policy and procedures for compliance in software development efforts.

Finding #29

The use of the Matrix X autocode generator for ISS software can lead to serious problems if the generated code and Matrix X itself are not subjected to effective configuration control or the products are not subjected to unit-level V&V. These problems can be exacerbated if the code generated by Matrix X is modified by hand.

Recommendation #29

NASA should ensure that thorough IV&V is conducted on all code produced by Matrix X, including any hand-coded modifications made to it, and that there is adequate configuration control on the code generated by Matrix X.

NASA Response to Recommendation #29

NASA agrees with the intent of the recommendation. IV&V will be performed on programs in accordance with the approach explained in our response to item 27a above. NASA is aware of the problems and concerns relating to Matrix X. Software changes that are made after auto-code generation, configuration management difficulties with hand-crafted changes after regeneration, code that appears different after auto-generation because of new variable name assignments, and new releases of the auto-coding tool itself are the principal areas of concern. These problems and concerns are considered to be inherent to auto-code generation tools. The NASA IV&V Facility in West Virginia will continue to evaluate the use of auto-code generators and the Matrix X generator tool specifically in order to better characterize these concerns and develop policies and procedures to better govern the use of auto-generated code. Some potential users of Matrix X have already been working closely with the NASA IV&V Facility on the issue of Matrix X and auto-code generation in general. The IV&V Facility will review program plans for programs that plan to incorporate an auto-generation tool and will assist in the development of guidelines to minimize the risks.

Regarding the Product Group 1 (PG1) use of Matrix X for developing the ISS Control and Data Handling software, NASA concurs with the concern over the configuration change control and the verification of the auto-coded software. The configuration control of all auto-coded software should be both at the model level and at the source code level. The prime contractor will be receiving both the models and the generated source and binary code from the PGs and will regenerate the source and binary code to ensure completeness and accuracy of the delivery.

Product Group 1 had problems late last year with unit testing of the flight software produced by Matrix X, but at that time they concluded that it was better to utilize a more modular design. Coincident with this, Product Group 1 also used Matrix X to build unit test drivers without impacting the unit under test. This procedure also includes the capability to test the units on the target hardware. These changes alleviate the NASA IV&V Facility's original concerns with Matrix X and unit testing.

The prime contractor is currently negotiating the wording for the PG1 Software Development Plan to implement these changes. The prime contractor has not yet begun looking at the older Product Group 3 (PG3) Software Development Plan to determine any additional changes needed. The NASA IV&V Facility's analysis of PG3's use of Matrix X did not generate any concerns. It should be noted that neither Product Group 2 nor the prime contractor use Matrix X for coding their software.

Finding # 30

NASA does not have procedures in place for documenting the firmware that is placed in ISS components, particularly for devices that were grandfathered from Space Station Freedom.

Recommendation #30

NASA should ensure that all firmware code, particularly that grandfathered from Space Station Freedom, is properly documented and archived for future reference. Further, NASA should ensure that it retains the rights to such software.

NASA Response to Recommendation #30

NASA agrees with the recommendation. Direction to deliver copies of the documentation (requirement, design, test, etc.) of the firmware controller software prepared as part of their software development process is being given to each vendor. A library will be established in the Software Development and Integration Laboratory (SDIL) at the Sonny Carter Training Facility. In addition, as part of the sustaining engineering activity, a plan is being developed to bring the qualification firmware controller units to the IV&V Facility and provide a capability to use these controllers instead of math models when required to support anomaly resolution or testing.

Finding # 31

There has been a marked improvement in the software development process for the ISS.

Recommendation # 31

By no means have all problems been solved, and there is still much to be done. Continue the focused efforts.

NASA Response to Recommendation #31

NASA agrees with the recommendation. A strong management focus on the software development process for the ISS will continue. These include weekly status

reports concerning the prime contractor and product group developments and strong interaction at the design and test reviews. To ensure progress does not slip, the prime contractor has initiated several activities, including additional shift work, new hiring, and developer/tester teaming arrangements.

D. AERONAUTICS

Finding #32

The well-planned consolidation of NASA flight research aircraft at the Dryden Flight Research Center has been put on hold by congressional mandates. This uncertain situation has prompted low morale and caused the loss of good people, which could well lead to flight safety problems.

Recommendation #32

The impasse between NASA intentions and congressional mandate must be resolved as soon as possible.

NASA Response to Recommendation #32

NASA is continuing to work with both the Administration and Congress on the consolidation of flight research aircraft. As always, safety of flight remains the "number one" priority in all our aircraft operations. We will cancel or postpone missions if staffing attrition or other problems impact operations. Most recently, the Office of Safety and Mission Assurance completed an assessment of aircraft operations at the Ames Research Center, where they found "an extremely talented and dedicated group of professionals who are committed to mission success and safety." Although staff has been declining, a number of aircraft have been decommissioned, thereby allowing a smaller staff to continue effective and safe operations.

Finding #33

The fan blades on the 40' x 80' x 120' wind tunnel at the Ames Research Center developed cracks after only 2,000 hours of operation. To preclude shutting down the tunnel for the 1 year required to procure and install a new set of blades, it was decided to repair the old blades while waiting for delivery of the replacements. The repair includes wrapping the root section of the blades, which eliminates the ability to detect crack growth by visual inspection.

Recommendation #33

NASA should ensure that a suitable inspection program, including frequent checks using nondestructive evaluation methods, is implemented.

NASA Response to Recommendation #33

As part of the fan blade repair at the National Full-Scale Aerodynamic Complex (NFAC), quality assurance and inservice inspection procedures are being developed and applied to ensure functionality of the repair. All blades are being visually examined to assess and establish their condition prior to the start of repair. Throughout the repair process, both ultrasonic and acoustic tap testing is being performed to determine adequacy of the crack fill, as well as the wrap lay-up quality and bonding. After placing back in service, periodic inspections using acoustic tap testing and a series of full-scale fatigue tests will be implemented to monitor and characterize void

growth. Based on these testing results, criteria for the periodic inspections, including frequency and size of indications, will be developed.

Finding #34

NASA's aeronautics research programs aimed at increasing aviation safety are having and will continue to have a significant positive impact on both military and civil flight operations. Several of these were in cooperation with other Government agencies, such as the Federal Aviation Administration.

Recommendation #34

NASA should continue to pursue aeronautics research programs, particularly joint efforts with other agencies, that will increase the safety of air operations.

NASA Response to Recommendation #34

In direct support of the White House Commission on Aviation Safety and Security, NASA has begun a major safety research initiative in partnership with the FAA, DoD, the National Weather Service, and the aviation industry. NASA will invest up to a half billion dollars over the next 5 years targeted at a strategic goal of reducing aircraft accident rates fivefold within 10 years and tenfold within 20 years. This initiative will include research to reduce human-error-caused accidents and incidents, predict and prevent mechanical and software malfunctions, and eliminate accidents involving hazardous weather and controlled flight into terrain.

E. OTHER

Finding #35

The Space Shuttle program has experienced some difficulties when stable work processes were altered to counter obsolescence or meet new environmental requirements. The simultaneous change in pressure sensitive adhesive and cleaning wipe in the RSRMs to meet environmental regulations is one example.

Recommendation #35

The Space Shuttle program should not alter long-established and stable processes without defining and completing an adequate test program. If changes in stable and well-characterized safety-related hardware and processes are being driven by environmental requirements, NASA should consider seeking waivers of these requirements rather than altering a proven design.

NASA Response to Recommendation #35

The SSP has been and is committed to not altering long-established and stable processes without defining and completing an adequate test program. The program has long had requirements governing the recertification of hardware in the event of either a hardware design change and/or a process change(s) that affect form, fit, function, safety, and/or reliability. However, the program has authorized a recent requirement change (reference PRCB Directive S071024DL) to provide a program-level review of all hardware and/or process changes whose certification is based solely on analysis. This requirement change necessitates a program assessment of the rationale for specifically defined changes whose recertification is based solely on an analysis, as opposed to those where the recertification is based on the performance of an adequate test program. It is felt that compliance with this new requirement will assure that changes to long-established and stable process changes are only implemented with adequate and appropriate recertification.

For any safety-related hardware or process change that is being driven by environmental requirements, NASA includes in its initial assessments the appropriateness of seeking a waiver to the requirements that are causing the change. Where such an assessment substantiates the appropriateness of a waiver, then that waiver shall be sought. The SSP adopted a policy that balances flight safety and environmental protection goals in SSP letter MS-96-071, dated September 16, 1996. The SSP manager specified: (1) obtain long-term waivers for materials essential to safe Space Shuttle operations where functionality cannot be verified; (2) obtain long-term waivers for materials where no replacements exist; and (3) continue to pursue identification and certification of replacement materials.

Finding #36

While firefighting preparedness and training in NASA is generally adequate, further reductions in staffing and funding may compromise the ability to perform this vital safety function.

Recommendation #36

Continue to review firefighting at all NASA Centers to ensure that funding, personnel, training, and adequacy of equipment are properly addressed.

NASA Response to Recommendation #36

NASA agrees with the assessment that fire protection for NASA facilities could suffer if not properly managed by NASA.

In accordance with NMI 1240.3, "Functional Management," the Office of Safety and Mission Assurance (OSMA) has performed functional reviews ("spot checks") at each Center since March 1994. Each of these functional reviews had, as an element, an evaluation of the fire protection program for the Center. In prior years, reviews were conducted as part of a Center survey process, which also included fire protection. These reviews focused principally on whether firefighting preparedness and training within NASA is at the appropriate level for performing this vital safety function.

Because of the recommendation made by the Panel, additional attention has been focused on this concern within NASA over the last several months. During the NASA Emergency Preparedness Coordinators meeting held at the Ames Research Center, February 25–28, 1997, all coordinators were given an action to further pursue this specific concern at their individual installations as a "high level of interest." At the May 21–23, 1997, meeting for NASA Fire Protection Coordinators, held at the Jet Propulsion Laboratory, these coordinators provided a "status" briefing on the posture of their fire protection program in light of the stated concerns by the Panel.

All NASA Centers and Installations have reported that their fire protection and response capability at this time remains adequate. However, it was a consensus that diminished NASA budgets have fostered a concomitant shifting of each NASA Center's reliance to the community's local fire protection and response capability through memoranda of agreement. Because local community fire departments are feeling the same pressure of downsizing that the Federal establishments are facing, these departments are also reducing capabilities and increasing response times. The OSMA, the Enterprise Institutional Program Officers (IPOs), and the Center Fire Protection Coordinators will need to be increasingly vigilant that any shift of local community fire department's response capability away from Federal facilities will not increase the risk to NASA personnel or property to an unacceptable level.

The OSMA will continue to focus attention on fire protection in our scheduled visits to Centers and will keep the Enterprise AAs and IPOs informed. Through proper assessment and advocacy for application of appropriate resources through the IPOs, we will continue to assure that NASA personnel and resources are afforded the highest degree of fire protection.

ATTACHMENT 1

Specific responses to Section III: Information in Support of Findings and Recommendations, #23, ASAP Annual Report, February 1997:

1. ***Auditory or visual locator for PCS units in an alarm condition.***
   RESPONSE: A PCS locator function is an interesting concept; however, the benefits of a beeping laptop need to be weighed against the ambiguity caused by several beeping laptops located in multiple locations throughout the vehicle. This capability as well as options pertaining to visual location will be studied for future upgrades.

2. ***Strategies to implement remedial actions from the PCS keyboard.***
   RESPONSE: The PCS is the primary crew interface device for ISS vehicle systems and payloads. This includes all required data and commands to operate the vehicle during nominal, assembly, and contingency situations. In this role, the PCS provides detailed C&W event information, confirming cues in the form of associated data, and complete response capabilities through commands initiation. The crew can also initiate emergency alarms manually from the PCS as well as automated responses to these events per Engineering Change Proposal (ECP) 555.

3. ***A localization scheme for depressurization events.***
   RESPONSE: Mission Operations personnel working in conjunction with the Flight Crew Office, Safety, Boeing prime contractor, and the CWSIT have developed isolation procedures for rapid depressurization events as well as many other contingency scenarios. These procedures and flight rules undergo much review and scrutiny during the stage specific Certification of Flight Readiness (CoFR) and Flight Readiness Reviews (FRR) processes. The procedure pertaining to rapid depressurization involves (a) proposed (ECP 555) automated software actions to isolate ventilation valves, overboard vents, and cabin air circulation, (b) manual crew hatch closures, and (c) the use of the PCS and module pressure sensors to isolate the leak to a specific module.

4. ***Interfaces with the ECLSS; division of responsibilities must be further defined.***
   RESPONSE: Since its introduction, the CWSIT has worked closely with the ECLSS architecture team to ensure common goals are met with respect to an integrated C&W system. The ECLSS has functional responsibility for the specifications pertaining to rapid depressurization, fire, and toxic spill, while the CWSIT has the responsibility of ensuring a safe, robust, and operationally integrated C&W system. ECLSS is one of many teams interfaced with by the CWSIT; others include all system architecture teams, safety, human factors, software design, operations, and the flight crew.

5. ***The control of payload toxic hazards, detection of fire, and power failure must be resolved.***

   RESPONSE: ISS payloads have stringent hazard control requirements, including automated safing, triple containment of hazardous substances, etc. Payload C&W events also undergo the same event classification process as ISS systems and will enunciate appropriate C&W events as required.

   Fire detection for the ISS is performed by an integrated system of rack and open volume sensors. These sensors are located throughout the vehicle and with all international modules. Response to a fire scenario is well documented and receives station, safety, flight crew, and mission operations program approval prior to flight.

   Loss of electrical power is detected by the power system and enunciated by the C&W system. Several automated Failure Detection, Isolation, and Recovery (FDIR) routines are contained with the vehicle software to respond to all but the most benign losses of power. Loss of main bus power, which causes a cascade effect, is controlled by proper C&W event classification and integration of C&W and FDIR algorithms.

6. ***The team needs to be given sufficient priority so that their systems engineering activities can have a timely influence.***

   RESPONSE: The CWSIT has been given full authority to review, guide, and recommend system changes for the C&W system. This includes official recognition of the organization within the Avionics Integration Office and charter as directed by the Deputy Program Manager for Operations. The CWSIT will continue to provide design integration expertise in a most prudent fashion, and without regard to organizational boundaries.

ATTACHMENT 2

Response #25: Specification to accommodate a "hands-free" communications capability on the International Space Station:

1. The Station Wireless Communications Subsystem (SWCS) shall provide wireless duplex voice communication over any one of the audio loops in the ISS Audio Distribution Subsystem.

2. The crew shall have the capability to receive, but not to originate, page messages over the SWCS (the crew would go to an Audio Terminal Unit, which has provisions to prevent acoustic feedback, to originate a page—no headset required).

3. The SWCS shall provide communications coverage throughout all inhabitable modules with hatches open or closed.

4. The SWCS shall have provisions to add the following capabilities at a later date:
   (a) two-way video synchronized with the audio channels to support video conferencing
   (b) data file transfers

5. The SWCS will be installed on orbit no earlier than assembly flight 6A.

Appendix C

AEROSPACE SAFETY ADVISORY PANEL ACTIVITIES JANUARY–DECEMBER 1997

JANUARY

6 Kennedy Space Center, STS-81 Flight Readiness Review

7–8 Kennedy Space Center, Review of KSC Operations and Space Flight Operations Contract

16 Johnson Space Center, Review of Space Operations with Thiokol Officials

30 Kennedy Space Center, STS-82 Flight Readiness Review

FEBRUARY

6–7 Headquarters, Aerospace Safety Advisory Panel Annual Meeting; Caution and Warning System, Aeronautics, Chief Information Office, and Ethics Briefings

10–11 Kennedy Space Center, STS-82 Launch and Discussions with Center Director

18 Johnson Space Center, International Space Station Caution and Warning System Briefing

24 Headquarters, Space Shuttle Related Topics with Associate Administrator for Space Flight

MARCH

5 Headquarters, Aerospace Safety Advisory Panel Planning Discussion with Staff

10–12 Kennedy Space Center, KSC Operations and Space Flight Operations Contract Update

13 Headquarters, Testimony Before the House Subcommittee for Space and Aeronautics

20 Kennedy Space Center, STS-83 Flight Readiness Review and Super Light Weight Tank Discussions with MSFC Center Director

26 Seattle, WA, The Boeing Company, International Space Station Discussions

27 Ames Research Center, Computer Hardware/Software Team Visit

APRIL

3 Lockheed, International Space Station 3rd Tier Discussions

17 Crystal City, VA, Space Flight Operations Contract (SFOC) Discussions with United Space Alliance Advisory Board

30 Kennedy Space Center, STS-84 Flight Readiness Review

MAY

6–8 Kennedy Space Center, KSC Operations and Plenary Session

12–13 Ames Research Center, Aeronautics Team Visit

22 Kennedy Space Center, NASA/FAA Human Factors Workshop

28 Headquarters, Meeting with Deputy Associate Administrator for Space Flight

JUNE

17–19 Marshall Space Flight Center, Review of Space Shuttle Projects/Reusable Launch Vehicle/Space Station Programs

19 Kennedy Space Center, STS-94 Flight Readiness Review

JULY

8–9 Langley Research Center, Aeronautics Team Visit

17 Sundstrand, Auxiliary Power Unit Sub-Task Team Visit

17 Hamilton Standard, International Space Station 3rd Tier Visit

24 Kennedy Space Center, STS-85 Flight Readiness Review

AUGUST

12–14 Johnson Space Center, Review of Space Shuttle, International Space Station, and Other Programs and Plenary Session

18 Headquarters, Space Shuttle Safety Study Status Review with Deputy Associate Administrator for Space Flight

SEPTEMBER

8 Headquarters, Review NASA Response to Annual Report
9 Headquarters, Human Exploration and Development of Space Assurance Board Video Teleconference
12 Kennedy Space Center, STS-86 Flight Readiness Review
15–16 Dryden Flight Research Center, Aeronautics Team Visit
17 Boeing-Rocketdyne, Space Shuttle Team Visit
18 Boeing, Space Systems, Space Shuttle Team Visit
23–25 Marshall Space Flight Center, Space Program Conference
25 Kennedy Space Center, STS-86 Launch
29 Fairmont, WV, to Discuss Independent Verification and Validation
30 Michoud, Visit to Discuss Super Light Weight Tank Design Certification Review

OCTOBER

1 Headquarters, Testimony Before the House Subcommittee for Space and Aeronautics
6 Kennedy Space Center, KSC/Space Flight Operations Contract Team Visit
16–17 Thiokol, Reusable Solid Rocket Motor Review

NOVEMBER

3 Kennedy Space Center, STS-87 Flight Readiness Review
4 Headquarters, Meeting with Congressman Sensenbrenner
18–19 Headquarters, Plenary Session and Preparations of Annual Report

DECEMBER

1–3 Headquarters, Editorial Committee Meeting
17–18 Johnson Space Center, JSC Task Team Visit
18–19 Headquarters, Editorial Committee Meeting